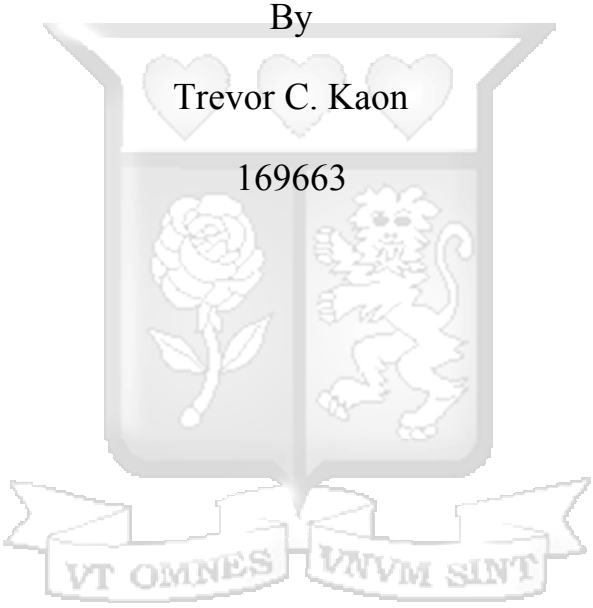
Gigabit Passive Optical Network Fraud Detection Via Realtime Optical Line Terminal Events Processing

By

Trevor C. Kaon

169663



Master of Science in Information Systems Security

2025

Gigabit Passive Optical Network Fraud Detection Via Realtime Optical Line Terminal Events Processing

By

Trevor C. Kaon

169663

Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Science in Information Systems Security at Strathmore University

School of Computing & Engineering Sciences

Strathmore University

Nairobi, Kenya

June, 2025

Declaration and Approval

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Student's Name: **Trevor C. Kaon**

Sign: _____ Date: 06-April-2025

Approval

The dissertation of **Trevor C. Kaon** was reviewed and approved for examination by the following:

Dr. Vitalis Gavole O.

Lecturer, School of Computing & Engineering Sciences,

Strathmore University

Sign: _____ Date: 7 April 2025

Abstract

Gigabit Passive Optical Networks (GPON) enables service providers to deliver high-speed broadband services to customers over fiber optic cables. GPON networks rely on Optical Line Terminals (OLT) to interface between the core networks and handle configuration of Optical Network Terminals (ONT) or Optical Network Units (ONU) which are situated at the customer premises. Malicious insiders at the Internet Service Provider (ISP) with access to network elements such as OLTs could abuse their access rights to perpetuate fraudulent activities. GPON fraud detection is the process of identifying and analyzing such attacks by analyzing the OLT events and alerting the relevant security incident response teams. This dissertation explores existing GPON security solutions and mechanisms. In addition, the dissertation implements an efficient mechanism for detection, analysis, visualization and alerting on suspected GPON fraudulent activities using open-source tools. The key methodology adopted by this dissertation is experimental prototyping in order to test the functionality of the mechanism and act as a proof of concept. The main output of this dissertation is a prototype that can be deployed on an enterprise fixed network served by an ISP. The developed solution can detect and alert on GPON fraudulent activities in real time hence reducing loss of revenue and ensuring a better and consistent quality of service to customers.

Keywords: *GPON, OLT, ONU, Wazuh, Fraud Detection, Fiber Optic, Intrusion Detection, Network Security.*

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
ARM	Access Resource Management
ATM	Asynchronous Transfer Mode
DBA	Dynamic Bandwidth Allocation
FPGA	Field Programmable Gate Array
GEM	GPON Encapsulation Method
GPON	Gigabit Passive Optical Networks
MFA	Multi-Factor Authentication
NMS	Network Management System
ODN	Optical Distribution Network
OMCI	ONU Management and Control Interface
ONU	Optical Network Unit
ONT	Optical Network Terminal
OLT	Optical Line Terminal
P2MP	Point-to-Multipoint
PPPoE	Point-to-Point Protocol over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SNI	Service Node Interface
SLAs	Service-Level Agreements
TACACS+	Terminal Access Controller Access-Control System Plus
T CONT	Transmission Container
TDM	Time Division Multiplexing
UNI	User Network Interface
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WDM	Wavelength Division Multiplexing
ZTP	Zero-Touch Provisioning

Definition of Terms

Gigabit Passive Optical Network	FTTH Council Europe (2024) defines GPON as a modern and widely adopted technology for provisioning of fast and reliable fixed Internet connectivity to homes or businesses commonly known as Fiber to the Home or Fiber to the Business respectively.
Optical Line Terminal	An OLT is the central network element in a GPON architecture located at the service provider's central office. The OLT manages the optical distribution network, controls ONU/ONT operations, allocates bandwidth, and enforces service policies (International Telecommunication Union, 2008).
Optical Network Unit /Optical Network Terminal	An ONU or ONT is a device situated at the end-user premises that converts optical signals received from the OLT back into electrical signals for user devices. It enables the delivery of internet, voice, and video services over fiber connections (Nathan Pan, 2023).
Optical Distribution Network	An ODN is the physical fiber optic infrastructure that connects the OLT to multiple ONUs/ONTs. It consists of fiber cables and passive optical splitters allowing point-to-multipoint connectivity (International Telecommunication Union, 2008).
Passive Optical Splitter	International Telecommunication Union (2008) defines a passive optical splitter as a device used in GPON networks that divides a single optical signal from the OLT into multiple signals to serve several ONUs without requiring electrical power.
Point-to-Point Protocol over Ethernet	PPPoE is a network protocol used to encapsulate Point-to-Point Protocol frames inside Ethernet frames. In GPON, PPPoE is widely used for user authentication, bandwidth management, and session control (Hongjian Guo, 2015) .

ONU Management and Control Interface	International Telecommunication Union (n.d.) defines OMCI as a protocol used by the OLT to manage and configure ONUs in GPON networks. It allows for remote provisioning, performance monitoring, and fault management.

Acknowledgement

The completion of this dissertation would not have been possible without the support of different individuals from diverse backgrounds. Special gratitude goes to Dr. Ozianyi for his valuable guidance during the process of writing this dissertation. I also extend appreciation to my colleagues and classmates for their valuable input. Finally, a special thanks to my family, who have supported me all through the journey.

Chapter 1: Introduction

1.1 Background to the Study

Gigabit Passive Optical Networks (GPON) is a modern and widely adopted technology for provisioning of fast and reliable fixed Internet connectivity to homes or businesses commonly known as Fiber to the Home or Fiber to the Business respectively (FTTH Council Europe, 2024)1. As depicted in Figure 2.1, GPON operates by transmitting high-speed broadband services from the service provider's core network to the customer's edge through a series of components where data is first aggregated and converted into optical signals by the Optical Line Terminal (OLT). These optical signals travel over a passive Optical Distribution Network (ODN) composed of fiber optic cables and passive splitters, reaching Optical Network Units or the Optical Network Terminal at customer premises. The Optical Network Unit (ONU) or ONTs convert the optical signals back into electrical signals facilitating the delivery of INTERNET, voice, and video services. The User Network Interface (UNI) marks the demarcation point, providing connectivity for Customer Premises Equipment (CPE) such as routers and computer (Nathan Pan, 2023) . Within GPON, OLTs control and manage most of the functionalities using Optical network unit Management and Control Interface (OMIC). OMIC enables activities such as ONU registration, bandwidth management and other service policy enforcements (International Telecommunication Union, 2022). However, like any technology GPON is susceptible to various fraudulent activities. Current research and existing GPON security solutions and mechanisms are not universally effective against fraud.

These solutions include mutual authentication, secure key establishment, and data encryption (Horvath et al., 2015). Another solution is the provisioning of centralized identity and access management on elements such as OLTs for single sign-on using protocols such as tacacs or radius (Cisco Systems, 2024). Alternatively, the use of Network Management system for GPON is recommended for centralized management of all GPON elements, network optimization, traffic monitoring, network alarms monitoring and timely deployment of security patches and firmware

[1]https://ftthconference.eu/visiting/what-is-ftth

updates (Huawei, 2023). Although centralized authentication systems are valuable for managing access and permissions, they are inherently limited in fraudulent cases whereby insiders already possess legitimate credentials and permissions within the network elements, granting them access to perform sensitive operations.

These systems have no capability to detect or prevent malicious activity in real time once an insider is authenticated. A significant limitation in many OLT Network Management Systems is the lack of customizable correlation rules which restricts the system's ability to detect and respond to nuanced or specific threat patterns. Without the capability to set tailored alerts based on custom criteria such as matching or excluding certain log patterns, the NMS is less equipped to identify insider threats or fraudulent activities in real time. This gap not only increases security risks but also adds operational strain, as manual oversight becomes necessary to catch potentially harmful anomalies that could otherwise be flagged automatically.

Due to limitations of current research and existing approaches, this dissertation developed a new approach that provides real time detection, analysis, visualization and alerting of suspected fraudulent activities.

1.2 Problem Statement

GPON are susceptible to various fraudulent activities, posing significant security risks. Fraudulent activities within GPON greatly impact revenue generation for the business and the network quality of service thus impacting customers. Current research and existing security solutions do not provide robust mechanisms for detection and real-time alerting of fraud related activities. Internet Service Providers need to conduct analysis of OLT operator events to acquire valuable insights into these activities and identify fraud. A solution that can implement real-time analysis and correlation of OLT events will reduce the risk of fraudulent activities.

1.3 Objectives of the Study

1.3.1 General objectives

This dissertation aims to develop a real-time fraud detection solution using operator activities on GPON OLTs.

1.3.2 Research objectives

i. To investigate characteristics of activities in GPON OLTs that may result to fraud,

ii. To analyze current research and existing GPON security solutions and mechanisms,

iii. To develop a solution to facilitate detection and alerting of fraudulent activities on GPON OLTs,

iv. To test the developed solution.

1.4 Research Questions

i. What are the characteristics of fraudulent activities on GPON OLTs?

ii. What are the current research and existing GPON security solutions and mechanisms?

iii. How does the solution to GPON OLT fraudulent activities operate?

iv. Is the solution able to identify fraudulent activities?

1.5 Scope and Limitations

This dissertation investigates operator activities performed on GPON OLTs that may result in fraudulent activities as a key objective. Moreover, it explores mechanisms for real-time monitoring, detection, visualization and alerting to the relevant incident response and management teams. The dissertation does not address mechanisms for preventing GPON related fraudulent activities. The solution is tested on an OLT manufactured by ZTE operating within a designated test environment. While the solution may have applicability in various environments, it is important to note that the research is limited to ZTE vendor based OLTs and access to OLTs from different vendors are not available.

1.6 Significance of Study

The potential of GPON fraudulent related activities on fixed internet service providers is high where insiders or internal employees with access to the management plane of GPON elements such as OLTs tend to abuse their access rights to initiate fraudulent operations. This impacts both the providers and customers negatively as it affects the business revenue and the quality of service. Therefore, the solution is important to the aforementioned establishments.

Chapter 2: Literature Review

2.1 Introduction

This chapter presents a review of the design and security of GPON technology. It also explores mechanisms for perpetuating fraudulent activities within GPON. Subsequently the chapter analyses current research and existing GPON security solutions and mechanisms. Finally, a conceptual framework depicting the solution is presented.

2.2 Technology Review

Gigabit Passive Optical Networks (GPON) deliver high-speed data transmission over fiber optic networks using passive infrastructure. The GPON standard ITU-T Recommendation G.984.1 defines a point-to-multipoint (P2MP) topology with asymmetric downstream and upstream capacities (ITU-T G984, 2008). By utilizing a point-to-multipoint topology, GPON networks enable a single optical fiber to connect multiple users reducing costs through passive optical splitters. However, the shared nature of GPON's infrastructure introduces significant security challenges particularly concerning the Optical Line Terminal (OLT) and Optical Network Units (ONUs) that facilitate management and data transmission across the network.

2.2.1 Architecture Design of GPON and Security Challenges

The GPON architecture comprises essential components including the OLT, ONUs, the Optical Distribution Network (ODN) and the User Network Interface (UNI). Each component plays a distinct role in the network's functionality and security.

The Optical Line Terminal is located at the service provider's central location and serves as the central management point within GPON. OLT relies on the OMCI to configure ONUs, allocate bandwidth and enforce service policies. Given its central role in managing network functions, the OLT is susceptible to unauthorized access where attackers could alter configurations, intercept data or degrade service quality.

Optical Network Units positioned at end-user locations convert optical signals from the OLT into electronic signals for user devices. ONUs employ Port-ID based filtering to ensure that only designated data reaches each ONU. However, Horvath et al. (2019) highlight that ONUs are vulnerable to identifier modification, where unauthorized devices clone legitimate identifiers to

intercept network data or modify configurations. Effective ONU authentication protocols are therefore essential for securing network integrity.

The Optical Distribution Network links the OLT to multiple ONUs through passive splitters allowing data to be distributed across a shared medium. While the ODN's passive structure reduces infrastructure costs, it limits security controls exposing downstream data to potential interception. Ajmal et al. (2007) recommends phase encryption methods that ensures data transmitted over the ODN is protected from unauthorized access and interception, thereby enhancing the overall security of the network. Additionally, Gutierrez et al. (2007) highlight the necessity of upstream encryption to prevent eavesdropping and other security threats ensuring that both downstream and upstream data are secured.

Finally, the User Network Interface connects the ONU to the end-user's internal network while the Service Node Interface (SNI) connects the OLT to the service provider's network. Although the UNI falls outside GPON's core, securing this interface is crucial as breaches here could expose user data to unauthorized access and compromise network integrity. Similarly, securing the SNI is essential to protect the broader network infrastructure. Together these components illustrate the need for a multi-layered security approach that addresses vulnerabilities across all network segments. Below is Figure 2.1 depicting High-Level Design of GPON.

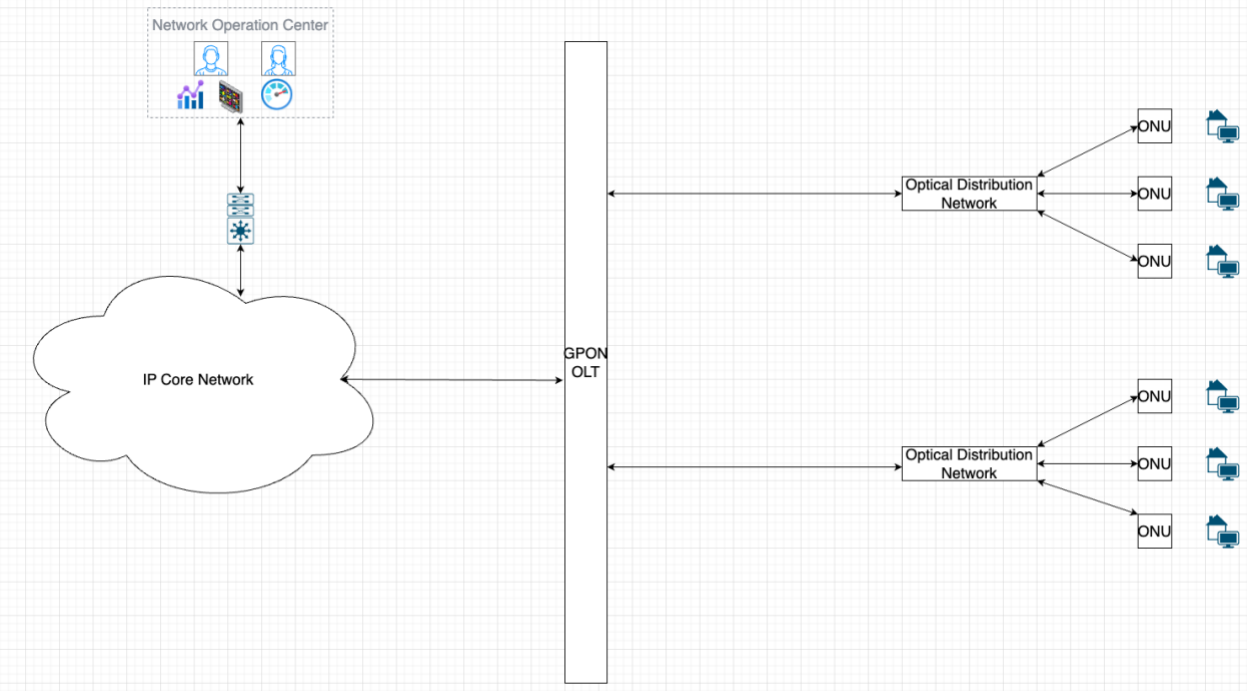


Figure 2.1: GPON High Level Design

2.2.2 Operation of GPON

The operational framework of GPON involves a range of technologies and mechanisms designed to facilitate efficient data transmission, resource allocation and service management. Key elements such as Time Division Multiplexing (TDM) and Wavelength Division Multiplexing (WDM), Dynamic Bandwidth Allocation (DBA), GPON Encapsulation Method (GEM), Transmission Containers (T-CONTs), Virtual Local Area Networks (VLANs), Service Profiles and PPPoE contribute to GPON's ability to deliver scalable high-speed services across a shared infrastructure. However, these mechanisms also introduce vulnerabilities that require rigorous security oversight.

GPON leverages both Wavelength Division Multiplexing (WDM) and Time Division Multiplexing (TDM) for efficient data transmission. WDM uses different wavelengths for bidirectional transmission, while TDM allocates time slots to ONUs ensuring orderly data flow. Wavelength Division Multiplexing is integral to GPON operations. In this system, downstream data is transmitted from the OLT to ONUs at a wavelength of 1490 nanometers, while upstream data travels at 1310 nanometers. As noted by Liu et al. (2011), WDM enhances data flow efficiency and minimizes interference ensuring seamless bidirectional communication. However, the shared broadcast model for downstream transmissions in traditional GPON presents a security risk, as

unauthorized ONUs can potentially intercept data by replicating valid Port-IDs. While advanced technologies such as WDM-PON and WRPON mitigate this risk by using wavelength segregation and dynamic routing to enhance security, these measures do not eliminate the need for robust ONU authentication and encryption mechanisms. Such safeguards are essential to address potential vulnerabilities and ensure secure operations in WDM-based GPON systems.

Time Division Multiplexing enables multiple data streams to share the same transmission medium by allocating unique time slots for each ONU to transmit data upstream to the OLT. TDM ensures efficient bandwidth utilization and minimizes data collisions but requires precise synchronization to maintain network stability and data integrity. Like WDM, TDM networks must adopt advanced security measures to prevent unauthorized access and ensure seamless operations.

Dynamic Bandwidth Allocation is a critical feature of GPON networks that enables the dynamic adjustment of upstream bandwidth allocations based on demand ensuring efficient resource utilization and prioritization of critical applications. The Optical Line Terminal regulates bandwidth among ONUs allocating resources to high priority applications such as Voice over IP (VoIP) and video streaming which require low latency and consistent performance. As noted by Yang et al. (2020), DBA algorithms enhance channel utilization and minimize delays hence ensuring Quality of Service (QoS) for diverse service categories. The flexibility of DBA mechanisms allows networks to accommodate fluctuating demand while maintaining service quality. However, they are susceptible to manipulation by malicious actors who may alter bandwidth allocations through unauthorized OMCI configurations. Such manipulations can monopolize bandwidth degrading service quality for other users. The authors emphasize that effective DBA algorithms should include safeguards to detect and mitigate anomalies in bandwidth usage patterns, such as unauthorized increases in allocations in order to prevent service disruption and maintain fairness across ONUs.

GPON Encapsulation Method is a critical mechanism used to encapsulate various types of data including Ethernet, IP and ATM frames for efficient transport across the GPON network. GEM ensures service differentiation and enables the transmission of diverse data formats within GPON. Each GEM frame includes a Port-ID for data flow identification and an error checking code for verifying data integrity. The GEM protocol facilitates data separation within the shared downstream communication model thus allowing the Optical Line Terminal to transmit data to the

appropriate Optical Network Unit based on its assigned Port-ID (ITU-T G 984, 2008). As noted by Selmanovic & Skaljo (2010), while GEM provides high encapsulation efficiency of 93% for upstream and 94% for downstream, it lacks built-in payload encryption leaving data vulnerable to interception. The multicast nature of GPON networks exacerbates this vulnerability as downstream transmissions can be intercepted by unauthorized ONUs. Addressing this limitation, implementing encryption within GEM frames could significantly enhance data security. However, such enhancements may introduce additional processing overhead potentially impacting network efficiency.

Transmission Containers play a vital role in GPON networks by categorizing upstream traffic based on priority levels thereby supporting the network's QOS requirements. T-CONTs enable the prioritization of high-importance applications such as real-time video conferencing or voice calls over lower priority data traffic ensuring that time sensitive services are delivered with minimal delay. ITU-T G 984 (2008) documents that T-CONTs are instrumental in managing network resources efficiently, allowing GPON to support diverse service categories while maintaining QoS standards. However, the flexibility of T-CONT configurations also presents security risks. Attackers may exploit vulnerabilities in T-CONT settings to prioritize unauthorized traffic effectively monopolizing upstream bandwidth and degrading QoS for legitimate users. Unauthorized access to T-CONT configurations is often facilitated by compromised OMCI settings which allow attackers to disproportionately allocate resources. Securing T-CONT configurations is essential to prevent resource abuse and maintain the integrity of GPON operations. This underscores the need for robust authentication mechanisms and real time monitoring systems to detect and mitigate unauthorized modifications to T-CONT allocations.

Service Profiles define the parameters and access levels for each ONU. These profiles specify QoS settings, available bandwidth and service priorities, ensuring that each ONU receives the appropriate resources in accordance with service level agreements. By customizing these parameters, service providers can tailor user experiences and maintain efficient network resource allocation. However, Service Profiles are a common target for malicious attacks. Unauthorized modifications to profile settings can enable attackers to gain access to premium services, manipulate bandwidth allocations or alter QoS parameters, leading to degraded service for legitimate users. As noted by Selmanovic & Skaljo, (2010), the manipulation of configuration

profiles poses a significant threat to network integrity and resource distribution. To mitigate these risks, implementing stringent OMCI access controls is essential. Regular auditing of profile settings to identify unauthorized changes combined with the encryption of OMCI communications can help safeguard Service Profiles from exploitation. Additionally, robust access control protocols such as multi-factor authentication and real-time monitoring further enhance the integrity of these profiles. By maintaining strict security practices, service providers can protect profile integrity thus ensuring equitable service distribution and the reliability of GPON networks.

Virtual Local Area Networks provide an essential layer of segmentation within GPON networks in enabling service providers to partition traffic for various service types or user groups. By assigning VLAN tags to specific data streams, service providers can efficiently manage traffic flows in facilitating the delivery of diverse services such as Internet, voice and video over the same physical infrastructure (Nathan Pan, 2023). VLANs not only enhance network performance by streamlining traffic management but also bolster security by isolating traffic and restricting inter-segment access. VLAN configurations must be carefully managed to prevent vulnerabilities. Improper VLAN setups such as overlapping VLAN tags or inadequate access controls can result in data leakage thus allowing unauthorized users to gain access to restricted segments. This poses significant risks particularly in networks supporting sensitive services or confidential data.

Point-to-Point Protocol over Ethernet is a foundational technology in GPON for authenticating users especially in scenarios requiring individual user credentials. As detailed by Hongjian Guo (2015), PPPoE enables the creation of unique user sessions within GPON's shared optical infrastructure. This capability supports service providers in efficiently managing bandwidth, tracking user activity, and implementing usage-based billing systems. The integration of PPPoE with GPON networks highlights its importance for session management. In a GPON setup, the OLT communicates with ONUs to establish PPPoE sessions facilitating secure connectivity. According to author, the OLT directs the ONU to configure PPPoE instances which include parameters such as user credentials and IP configurations, ensuring a secure and stable connection. This configuration process ensures that the ONU can establish virtual connections with the Broadband Remote Access Server (BRAS), enabling robust authentication and data routing. However, PPPoE accounts are vulnerable to misuse, particularly by malicious insiders or external attackers who gain access to credentials. Huawei (2023) emphasizes the critical need for secure

authentication mechanisms and robust encryption protocols to prevent unauthorized access. Without these safeguards, attackers can exploit unencrypted credentials exchanged during the PPPoE handshake process, resulting in unauthorized access, service disruptions, or data theft. By combining secure authentication practices, robust encryption and real-time monitoring, service providers can mitigate the risks associated with PPPoE .

2.3 Characteristics of GPON Suspicious Fraudulent Activities

The shared and centralized nature of GPON infrastructure combined with its dependence on the OLT for network control makes it susceptible to various fraudulent activities. These activities not only compromise network security and data privacy but can also significantly impact service quality and revenue. While external attackers pose significant risks, insider threats are particularly concerning in network environments due to the privileged access that network operators and administrators have. A report by Resecurity highlighted the circulation of hundreds of network operators' credentials on the dark web (Resecurity, 2024). Malicious insiders such as rogue operators or technicians can exploit their authorized access to carry out fraudulent activities undetected. Key characteristics of suspicious fraudulent activities within GPON may include rogue ONU registration, profile policy manipulation (bandwidth manipulation) and service account misuse.

Rogue ONU registration is a security concern in GPON networks wherein unauthorized Optical Network Units are introduced into the network by replicating valid ONU identifiers such as serial numbers or authentication credentials. These fraudulent ONUs exploit the broadcast nature of GPON communication to intercept traffic intended for legitimate ONUs. This type of attack becomes particularly critical when carried out by malicious insiders who have privileged access to the OLT configuration. Insiders can bypass standard authentication mechanisms to register rogue ONUs thereby enabling them to intercept network traffic, modify configurations or leverage network resources for unauthorized purposes. The challenge of detecting rogue ONUs is compounded by GPON's shared infrastructure where all downstream data is accessible to every connected ONU. As emphasized by Horvath et al. (2019), a modified or rogue ONU can disrupt communication by violating time-slot assignments or impersonating legitimate ONUs through fake identifiers. This not only compromises data confidentiality but also degrades the quality of service for legitimate users across the network. To address these vulnerabilities, implementing

robust countermeasures such as regular auditing of ONU registration patterns, enforcing strict role-based access controls and encrypting OMCI communications can significantly reduce the risk of rogue ONU registration. Alarm mechanisms that monitor unusual activities such as time-slot violations provide additional safeguards for early detection and response ensuring the security and reliability of GPON networks.

Profile policy manipulation refers to the unauthorized alteration of parameters that define QoS settings, service priorities and bandwidth limits for ONUs. Bandwidth manipulation is an example of policy manipulation which involves the modification of Dynamic Bandwidth Allocation configurations to allocate disproportionate bandwidth to certain ONUs. As highlighted by Liwei et al. (2020), DBA is essential for ensuring efficient resource utilization, but its misconfiguration can lead to service disruptions. Malicious operators may exploit this to prioritize unauthorized ONUs or services degrading QoS for legitimate users. Furthermore, profile manipulation can involve altering QoS policies to grant unauthorized service levels, monopolizing network resources or favoring rogue ONUs. Such actions compromise the integrity of GPON networks and create unbalanced resource distribution leading to poor service delivery. Regular reviews of profile and bandwidth allocation settings along with strict role-based access controls and real-time anomaly monitoring are critical to mitigating these risks.

Broadband remote access server is a critical component in broadband networks, playing a vital role in aggregating user sessions from access networks such as GPON and routing traffic to and from the internet. In addition to its traffic management responsibilities, the BRAS handles key functions such as user authentication, authorization, and accounting, often interfacing with RADIUS servers to manage these tasks. Huawei (2023) acknowledges the centrality of BRAS in facilitating subscriber connectivity and ensuring the integrity of network operations through robust authentication mechanisms. The integration of BRAS with GPON architecture underscores its importance in enabling high-speed broadband delivery to multiple subscribers through a shared optical infrastructure. Hongjian Guo (2015) explains that the BRAS serves as a pivotal gateway in this architecture, managing IP configurations and user authentication for numerous endpoints connected via OLTs and ONUs. This integration while efficient also amplifies the potential impact of credential misuse. Misuse of BRAS credentials often stems from vulnerabilities such as weak or default passwords, unencrypted credential in configuration or exchanges during the PPPoE

handshake process and outdated firmware. Gal Zror (2022) states that these weaknesses create significant attack vectors, especially in GPON environments where BRAS systems are responsible for managing large volumes of subscriber connections. An attacker exploiting these vulnerabilities can gain unauthorized access, intercept subscriber data or disrupt services through denial-of-service attacks. The reliance of BRAS on RADIUS servers for AAA functions also means that compromised credentials can have cascading effects, including unauthorized session hijacking or large-scale service outages. Attackers can impersonate subscribers to access sensitive data or modify session parameters, leading to degraded performance or complete service disruption.

To address these challenges, ISPs must adopt a multi-layered approach to securing BRAS credentials. Huawei (2023) recommends implementing strong authentication protocols, such as Challenge Handshake Authentication Protocol (CHAP) and ensuring encryption during PPPoE exchanges to prevent interception. Regular firmware updates are essential to address known vulnerabilities, while segmentation between subscriber and administrative interfaces can limit the attack surface. Gal Zror (2022) also highlights the importance of real-time traffic analysis and network monitoring to detect and mitigate unauthorized access attempts. Additionally, improvements in threat detection systems and automation in response mechanisms can further bolster the resilience of BRAS and GPON systems. By implementing these measures, ISPs can protect their infrastructure, safeguard subscriber data and maintain reliable service delivery in an increasingly interconnected broadband environment.

2.4 Assessment of Current Research and Existing GPON Security Solutions

Current Research and existing GPON security mechanism have identified a range of solutions designed to address vulnerabilities in authentication, data encryption, bandwidth management and network monitoring. However, these measures often have limitations in terms of scalability, real-time responsiveness and comprehensiveness especially in addressing complex insider threats and sophisticated external attacks. This section evaluates current research and industry solutions, critiquing their strengths and weaknesses and highlights existing gaps that warrant further research and development to ensure robust security in GPON networks.

2.4.1 Authentication and Access Control Mechanisms

Authentication and access control are fundamental to the security of GPON networks in ensuring that only authorized ONUs and users gain access to network resources. ONU authentication, a primary security measure, involves verifying each ONU's identity before allowing it access to the network. Standard authentication methods rely on serial number-based and key-based mechanisms which match ONUs to pre-registered serial numbers stored in the OLT database. While these methods provide a basic level of security, they are vulnerable to spoofing and cloning attacks. Attackers who replicate valid serial numbers can gain unauthorized access to network resources, highlighting the limitations of relying solely on serial number-based authentication. ONU authentication is strengthened by enhanced authentication mechanisms such as multi-factor authentication (MFA) which combines serial numbers with additional verification factors such as passwords (Cisco Systems, 2020).

To further enhance authentication, Malina et al. (2015) propose incorporating cryptographic techniques into the ONU registration process. By using unique cryptographic keys for each ONU and leveraging challenge-response protocols during registration, the authentication process becomes significantly more robust. This approach ensures that even if serial numbers are intercepted, they cannot be reused without the corresponding cryptographic key. Additionally, the authors emphasize that the integration of encryption with authentication protocols is essential for protecting communication channels and mitigating risks associated with data interception during the registration process. While cryptographic authentication mechanisms enhance security their implementation requires processing overhead and may pose scalability challenges in large-scale GPON deployments.

Centralized identity management protocols such as TACACS+ and RADIUS play a pivotal role in managing GPON access control. RADIUS operates as a protocol to authenticate, authorize and account for users accessing network devices. According to ZTE (2024) RADIUS servers authenticate operators or administrators remotely connecting to the OLT by validating user credentials and authorizing access based on predefined permissions. This centralized approach simplifies management and improves security by ensuring consistent access policies. TACACS+, an advanced access control protocol offers additional functionality over RADIUS. Developed as an enhancement to the TACACS protocol, TACACS+ separates authentication, authorization and

accounting functions, allowing granular control over each. The ZTE documentation emphasizes that TACACS+ encrypts all packet exchanges between the OLT and the server ensuring data security during transmission. Its use of TCP for reliable communication and its extensibility for site-specific customization further strengthen its utility in GPON environments. Additionally, TACACS+ enables dynamic authorization granting or restricting specific permissions based on real time operational needs which is particularly advantageous in mitigating insider threats.

Despite their strengths, both RADIUS and TACACS+ systems have limitations. Single points of failure in centralized systems pose significant risks if authentication servers are compromised. To address this, redundancy in authentication server deployment is essential to ensure high availability and minimize downtime. Furthermore, these protocols may introduce latency and operational complexity particularly for smaller networks where resources are limited. For small-scale deployments, the cost and complexity of deploying centralized systems such as TACACS+ and RADIUS can be prohibitive. Lightweight alternatives that incorporate MFA and secure communication protocols could offer a practical solution. Overall, access control mechanisms while effective in mitigating some external threats often lack scalability and fail to address internal threats posed by malicious insiders with legitimate access credentials.

2.4.2 Data Encryption Mechanisms

Data encryption is a cornerstone of GPON security, critical for preventing unauthorized interception of transmissions within the Optical Distribution Network (ODN) where downstream data is broadcast across a shared medium. Encryption mechanisms ensure that even if data is intercepted, it remains inaccessible without the corresponding decryption keys. This is especially important given the broadcast nature of GPON which makes it inherently vulnerable to eavesdropping attacks.

The Advanced Encryption Standard (AES) is widely employed for encrypting GPON data streams. Vinh et.al (2008) emphasize that AES integration with Field Programmable Gate Array (FPGA) modules enhances encryption efficiency by providing low-latency protection and high-speed data processing. This hardware-based solution significantly outperforms traditional software encryption methods making it suitable for large-scale GPON deployments. However, the implementation costs associated with FPGA-based encryption pose challenges for smaller networks or budget-constrained service providers limiting its adoption.

To address the cost and scalability challenges, researchers have explored alternative methods. Ajmal et al. (2007) propose phase encryption as a viable alternative, which secures data using optical phase shifts. Phase encryption offers robust protection while minimizing computational overhead making it suitable for specific use cases. However, it has scalability limitations and is better suited for specialized networks rather than large GPON deployments. Furthermore, its reliance on precise optical configurations reduces its adaptability in dynamic network environments highlighting the need for hybrid encryption solutions that balance cost, performance and scalability.

Existing encryption solutions focus on payload security often neglecting the protection of control channels like the ONU Management and Control Interface (OMCI). OMCI oversees critical network operations including ONU configuration, bandwidth management and service provisioning. Unauthorized access to OMCI could allow attackers to manipulate ONU configurations, alter bandwidth settings, or disrupt service profiles, posing severe risks to network stability.

2.4.3 Network Management Systems for GPON Networks

Network Management Systems (NMS) are essential tools for maintaining the operational stability and security of GPON networks. By providing centralized control, monitoring and advanced security features, NMS platforms enhance the overall security posture of GPON infrastructures.

Prominent examples of NMS solutions include ZTE's NetNumen U31, Huawei's iManager U2000 and iMaster NCE-FAN, each offering a range of features that address different operational requirements. NMS platforms enforce robust access control mechanisms such as role-based access control (RBAC) to ensure that only authorized personnel can make changes to the network. For instance, ZTE's NetNumen U31 and Huawei's iManager U2000 support multi-level access control, restricting access based on user roles and responsibilities. These platforms also integrate with centralized authentication protocols like TACACS+ and RADIUS, which authenticate users remotely and ensure consistent access policies across the network. Additionally, authentication logs maintained by the NMS record login attempts including failed attempts, aiding in the detection of unauthorized access (Huawei, 2013; ZTE, 2021). NMS platforms incorporate real-time monitoring and anomaly detection. Huawei (2021), employs intelligent alarm analysis to detect deviations in network behavior that may indicate security breaches.

NMS platforms enforce security policies across GPON networks by managing configurations at the OLT level. NMS like Huawei iMaster NCE-FAN enable automated provisioning of ONUs through Zero-Touch Provisioning (ZTP), reducing the likelihood of human error and insider threats. Additionally, monitoring and securing OMCI communications protect against unauthorized changes to bandwidth allocations and service profiles. These measures ensure that network operations remain compliant with established security standards and policies.

Event logging is a critical function of NMS platforms in facilitating detailed tracking of system operations, user actions and security events. Event logs are typically categorized into system logs, operation logs and security logs. System logs monitor routine events such as performance metrics and hardware statuses, while operation logs record user activities including configuration changes and command executions. Security logs capture incidents like failed login attempts, unauthorized access attempts and policy violations which are essential for forensic analysis and regulatory compliance. Platforms like NetNumen U31 provide granular filtering and role-based access to logs in enhancing the effectiveness of forensic investigations and security audits. NMS platforms contribute to regulatory compliance by maintaining transparent records of network activities. Detailed audit trails provided by systems like Huawei iManager U2000 enable administrators to track and verify adherence to internal and external security standards. Regular auditing of system logs, operation logs and security logs ensures that GPON networks remain compliant with evolving regulations and industry best practices. Table 2.1 provides a comparison of NMS Event log management features.

Table 2.1: Comparison of NMS Event Log Management

Feature	NetNumen U31 R18	Huawei iMaster NCE-FAN	Huawei iManager U2000
System Logs	Records essential system events, errors, and operational status changes. Can filter logs based on event type and importance.	Monitors system stability, hardware statuses, and performance metrics. Logs can be centrally stored and viewed.	Tracks extensive system events and provides a centralized storage and retrieval system for enhanced system monitoring.
Operation Logs	Records user activity with timestamps and details of commands and configuration	Logs all user operations, including remote configurations and ONT provisioning tasks. Supports a	Tracks all operational commands, configuration changes, and user actions for compliance and detailed auditing.

Feature	NetNumen U31 R18	Huawei iMaster NCE-FAN	Huawei iManager U2000
	changes. Maintains detailed audit trails.	detailed history view for audit purposes.	
Security Logs	Maintains logs of security events like login attempts, failed access, and system alerts. Supports role-based log access to enhance security.	Monitors access attempts, credential checks, and security policy violations. Logs can trigger alerts for critical security events.	Comprehensive security logging, capturing unauthorized access attempts, login failures, and successful/failed authentications. Supports compliance and forensics.

2.5 Identified Gaps in Current GPON Security Solutions and Mechanisms

Despite significant advancements in GPON security, existing solutions reveal several critical gaps that limit their effectiveness in addressing evolving threats. Authentication mechanisms, data encryption methods and Network Management Systems all exhibit limitations that compromise their ability to provide comprehensive and adaptive security.

Authentication mechanisms, while foundational are not robust enough to address all vulnerabilities. Centralized systems like TACACS+ and RADIUS remain susceptible to insider threats where malicious operators with legitimate credentials can exploit their access rights. Furthermore, these systems introduce single points of failure if the authentication server is compromised or unavailable the entire network becomes vulnerable to unauthorized access. Scalability is another issue as methods such as multi-factor authentication (MFA) and cryptographic protocols often impose processing overhead making them unsuitable for large-scale networks or resource-constrained deployments. Additionally, the financial and technical investment required for implementation creates barriers for smaller service providers. Current authentication mechanisms also lack real-time monitoring capabilities when they focus primarily on verifying access without proactively detecting ongoing unauthorized activity.

Data encryption mechanisms, though essential also show notable limitations. Many encryption solutions, such as FPGA-integrated AES focus primarily on securing payload data while neglecting the protection of control channels like the ONU Management and Control Interface. This oversight leaves critical network operations vulnerable to manipulation such as altering ONU configurations or service profiles. While FPGA-based encryption provides high performance, its cost limits accessibility for smaller operators. Alternative encryption approaches such as phase

encryption offer reduced computational overhead but lack scalability and adaptability to dynamic GPON environments. In addition, robust key management protocols essential for secure encryption are often absent hence increasing the risk of key compromise.

Network Management Systems play a vital role in GPON security but face significant limitations that hinder their effectiveness. NMS platforms tend to be reactive focusing on fault detection and performance monitoring rather than proactive threat identification. A significant shortfall in many OLT NMS platforms is the lack of customizable correlation rules which restricts the system's ability to detect and respond to nuanced or specific threat patterns. Without the capability to set tailored alerts, the NMS is less equipped to identify insider threats or fraudulent activities in real time thus increasing security risks and operational strain. The absence of customizable correlation rules introduces four critical challenges. First, reduced incident responsiveness arises as the NMS cannot automatically escalate or highlight certain log events that match critical patterns. This limitation delays incident response, requiring manual log reviews and increasing network downtime. Second, limited contextual alerting restricts the NMS to predefined generic alarms which cannot address nuanced scenarios or adapt to the unique requirements of specific networks. Third, increased operational overhead results as network operators must manually sift through large volumes of logs to detect significant events. Without automation, this labor-intensive process becomes error prone and inefficient. Lastly, limited adaptability to evolving threats and compliance needs prevents the NMS from responding dynamically to new attack patterns or changes in regulatory requirements, leaving the network vulnerable to emerging risks and non-compliance.

Although some advanced NMS platforms, such as Huawei iMaster NCE-FAN, incorporate intelligent alarm analysis and role-based access controls, they still prioritize operational metrics over comprehensive security. Additionally, while these platforms maintain detailed logs of system, operation and security events. The lack of advanced filtering and analysis tools reduces their utility in forensic investigations.

In Summary the gaps in GPON security mechanisms underscore the need for scalable, cost-effective and adaptive solutions to address both internal and external threats. Incorporating customizable correlation rules is essential for detecting nuanced threats, improving incident

responsiveness and reducing operational overhead. Addressing these challenges is critical to ensuring the security and adaptability of GPON networks in an evolving threat landscape.

2.6 Conceptual Framework

This research develops an integrated solution leveraging advanced log monitoring, centralized analysis, visualization and real-time alerting to suspicious operator events in GPON networks. The solution begins with data collection and preprocessing where log events from OLTs are gathered in real time. These logs encompassing operational command logs capture vital activities such as suspicious configuration changes. The preprocessing stage is powered by custom Wazuh decoders which utilize flexible regular expressions set to extract critical field attributes from raw log events. This ensures that irrelevant data is filtered out focusing the analysis on actionable insights. Wazuh decoders built on XML-based configuration files allow administrators to tailor log parsing rules to meet the specific needs of GPON infrastructure thus providing a higher level of granularity than Network monitoring systems.

Once parsed, the data advances to the event detection and analysis stage powered by a centralized Wazuh server. This server employs Wazuh indexer for efficient data indexing and Wazuh dashboard for real-time visualization. Wazuh indexer's distributed nature ensures scalable data storage and retrieval, while its indexing capabilities enhance the speed and accuracy of search operations. Predefined rules and advanced correlation algorithms are used to analyze the parsed logs, enabling the detection of anomalies. By analyzing patterns and correlating events, the server distinguishes between isolated incidents and coordinated attack patterns. This capability reduces false positives and enhances the accuracy of identification.

Visualization tools integrated into the Wazuh server such as dashboards display GPON specific metrics which enables administrators and security teams to monitor network health and detect suspicious activities proactively. These dashboards provide insights into event frequency and affected network elements presented in an intuitive and accessible format. This layer of visualization enhances situational awareness which allows for proactive identification and mitigation of potential security breaches before they escalate.

The final stage of the framework involves real-time alerting and collaborative incident management through Slack bot integration. Alerts are automatically generated by the Wazuh server and routed to designated Slack channels via Slack's Webhook API. The alerts include

detailed information about security events such as timestamps, affected OLTs and the severity level of incidents. The Slack bot prioritizes alerts based on their criticality hence ensuring that high impact threats are addressed promptly.

Slack's collaborative capabilities enable incident response teams to centralize communication, share insights and document actions in real time. Teams can annotate alerts with investigative findings, coordinate responses and maintain a historical record of each incident for post-event analysis. This historical data allows for the refinement of detection rules and response protocols thus improving the system's overall effectiveness. Figure 2.2 provides a visualization of the conceptual framework.

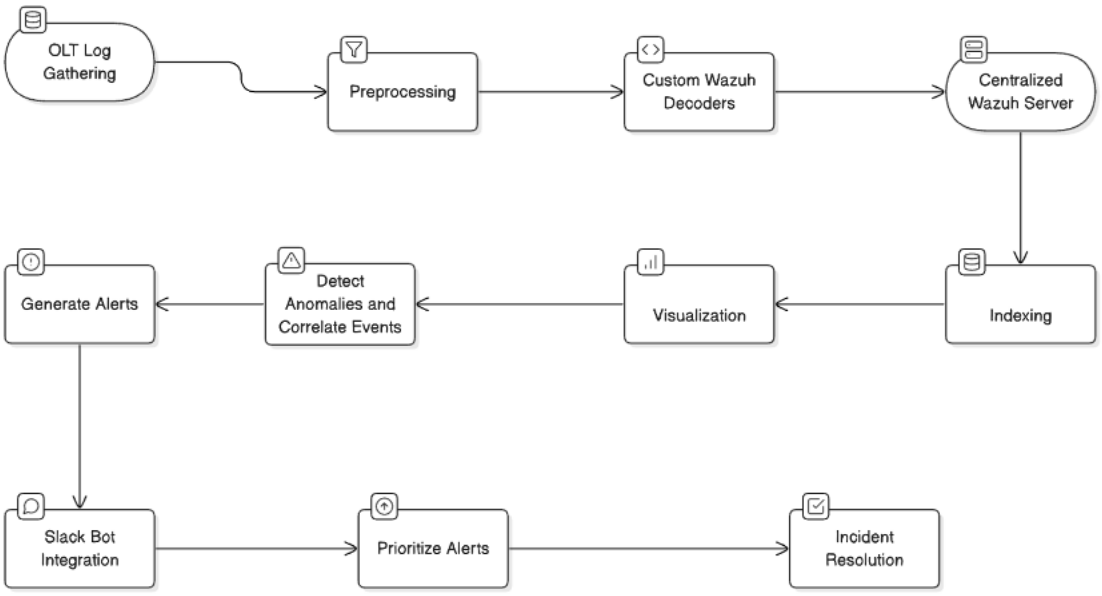


Figure 2.2: Conceptual Framework

2.6.1 Enhancing Existing Technologies

The solution enhances existing technologies in several ways:

i. Custom Wazuh Decoders

These decoders improve traditional log monitoring by NMSs tailoring event parsing to GPON-specific contexts. Unlike standard NMS which often use generic preconfigured rules, custom decoders isolate nuanced GPON related events.

ii. Wazuh Server

While NMS focus on predefined rules, this solution incorporates dynamic detection thresholds. These adaptive thresholds enable the system to recognize evolving attack vectors without requiring manual updates.

iii. Visualization

The use of Wazuh dashboard elevates the interpretability of data by offering GPON-specific visualizations that are not available in standard network monitoring platforms. This enables operators to configure custom dashboards to monitor custom metrics.

iv. Slack Integration

Existing alerting tools often lack real-time collaboration features. By integrating Slack, this solution bridges the gap between detection and response, allowing for coordinated, immediate action. The prioritization and documentation capabilities ensure efficient resource allocation during incident handling.

Chapter 3: Methodology

3.1 Introduction

This chapter outlines the methodology applied in designing, developing and testing a prototype solution to detect, analyze, and alert suspected fraudulent activities within GPON networks. The approach emphasizes a structured system development process, integrating event-driven detection and real-time alerting functionalities using tools such as Wazuh and Slack, deployed on an isolated GPON testbed. This methodology guides the project through stages of requirements analysis, design, implementation, testing and validation to ensure the solution is effective, reliable and ethically compliant.

3.2 Research Design

This dissertation adopts a prototyping research design involving testbed development to support experimental validation of the solution. The prototyping approach involves creating a functional testbed to evaluate the security mechanisms in a controlled environment which allows for experimentation and validation of the solution's detection and alerting capabilities. This design enables continuous feedback during development and testing phases in order to ensure that the system can effectively address identified security threats and achieve its intended objectives.

3.3 System Development Methodology

The system development methodology entails the following key sections: Requirements analysis, system design, implementation, testing and validation. This methodology ensures that the solution is built systematically from identifying functional requirements to final validation in a test environment.

3.3.1 Requirements Analysis

Requirements for developing the GPON security solution were identified based on a detailed assessment of the GPON's architecture, and the specific functionalities needed to detect and alert suspicious activities.

3.3.1.1 Functional Requirements

i. Event Logging and Publishing Requirements

The OLT must be capable of logging relevant events, such as command entries. These logs serve as the primary data source for detecting and analyzing suspicious activities.

ii. Event Ingestion and Parsing Requirements

Custom Wazuh decoders is configured to parse specific fields in OLT event logs responsible for identifying activities such as configuration changes.

iii. Detection, Analysis and Alerting Requirements

Wazuh deployed on an Ubuntu server provides the necessary framework for real-time detection and visualization of suspicious events. Integration with Slack facilitates immediate alerting and ensuring that incident response teams are notified promptly.

3.3.1.2 Non-Functional Requirements

Beyond functionality, the system must meet specific performance criteria to be effective:

i. Performance Requirements

The Wazuh server must operate within acceptable CPU, memory and disk input and output operations under baseline and peak loads. Monitoring of these resources is essential.

3.3.2 System Design

The System Design phase involves conceptualizing and structuring each component of the solution to ensure that it effectively addresses the identified security requirements. Design tools, including UML diagrams and network diagrams are utilized to model the interactions between the components using draw.io.

3.3.3 Implementation

The solution is implemented as a proof-of-concept testbed with a real test ZTE GPON OLT. Wazuh is deployed on an ubuntu server and is used for detection, analysis, visualization and alerting. A Slack bot is used to receive alerts from Wazuh and push notification to respective incident response and management teams. Performance tools are used to collect and visualize performance metrics.

The following steps are taken:

i. OLT Event Logging Configuration

The ZTE GPON OLT is configured to log specific event types, such as cmdlog and to forward the events to the wazuh server.

ii. Deployment of Wazuh on Ubuntu Server

The Wazuh server is installed on an Ubuntu operating system configured to receive and analyze event logs from a real test ZTE GPON OLT. Custom decoders are deployed within Wazuh to ensure accurate parsing and identification of security events. Alert rules are configured to match GPON fraud activities.

iii. Integration of Slack for Alert Notification

A Slack bot is configured with Wazuh's Webhook API which ensures that alerts generated by the Wazuh server are delivered to specified Slack channels. This integration allows the incident response team to receive real-time notifications on critical activities such as rogue ONU registrations or service account misuse.

iv. Integration of Performance Monitoring tools

To monitor the performance and resource utilization, Telegraf is installed as an agent on the Ubuntu server to collect system metrics such as CPU, RAM, disk I/O and OpenSearch performance at regular intervals. These metrics are sent to InfluxDB for visualization. This setup allows for tracking the performance impact of log ingestion, analysis and alerting

3.3.4 Testing and Validation

Testing and Validation are critical to assessing the solution's ability to identify fraudulent activities within GPON. The testing phase involves emulating various suspicious activities on the test ZTE OLT to generate event logs which Wazuh then analyzes. Testing activities include:

i. Simulating Suspicious Operator Activities

To test the detection capabilities realistically, custom Python scripts are developed utilizing the Netmiko library. These scripts are designed to automate SSH connections to the ZTE OLT and execute command sequences programmatically. These sequences mimic various operator activities including those previously identified as suspicious or potentially fraudulent thereby generating the necessary log events for Wazuh to detect and analyze.

ii. Evaluating Detection and Alerting Capabilities

Each simulated event is monitored to confirm that Wazuh decoders correctly identifies and parses the suspicious activity which triggers an alert based on the specified alert rules. The corresponding alert is forwarded by the Slack bot to the monitoring channel for real-time notification.

The validation process focuses on verifying that the system reliably detects and alerts on fraudulent activities thus ensuring its efficacy in a GPON test environment.

The following metrics guide the evaluation of the system's detection and alerting capabilities:

a. Detection Accuracy

This measures how well the system identifies actual fraudulent activity based on the predefined custom decoders and alerting rules.

b. Detection Latency

This assesses the time taken to detect and generate alerts from the moment the event occurs.

3.4 Data Collection and Sampling

The study collects real-time simulated data from OLT in a test environment depicting the ISP network. Purposeful sampling is adopted to ensure the system is tested on relevant data that reflects real-world GPON activities prone to manipulation such as rogue ONU registrations.

The sample size for testing is a minimum of five events for each simulated fraudulent activity. This size ensures a variety of normal and fraudulent activities. Logs are collected over simulated operational period of one day to include routine operations and fraud scenarios.

3.4.1 Inclusion and Exclusion Criteria

The following inclusion and exclusion criteria guide data collection:

Inclusion Criteria:

i. OLT events related to ONU registrations, policy changes and PPPoE account configurations.

Exclusion Criteria:

i. Non-GPON infrastructure logs such as unrelated routers or general IT systems.

ii. Environmental logs like temperature or voltage readings unrelated to fraud detection.

iii. Corrupted or incomplete logs that cannot be parsed or do not provide meaningful insight.

This ensures that the dataset remains focused on fraud-relevant events, enhancing the prototype's detection accuracy.

3.5 Data Analysis

The research utilizes mixed data analysis.

3.5.1 Quantitative Analysis

Quantitative data is statistically analyzed to determine the effectiveness of the detection mechanisms. Metrics such as detection rates and latency are examined using statistical methods to derive performance measures for the detection framework. Detection rate is calculated as the percentage of simulated suspicious activities that successfully trigger the corresponding Wazuh alert while alerting latency is measured as the time elapsed from the execution of a suspicious command to the delivery of the corresponding alert notification in the designated Slack channel.

Descriptive statistics is used to summarize these performance metrics across multiple test runs. while inferential statistics helps determine the statistical significance of observed differences.

3.5.2 Qualitative Analysis

A detailed review of the simulated fraud cases is conducted to assess the system's ability to correctly interpret event patterns. Manual validation is used to refine detection rules and reduce false positives.

3.5.3 Visualization

Key results such as detection accuracy rates and average alerting latency are summarized and presented using tables for clear comparison and interpretation.

Performance data collected by Telegraf (e.g., Wazuh server CPU usage, memory utilization, disk I/O) and stored in InfluxDB are visualized. Dashboards created using InfluxDB display these metrics over time, allowing for the assessment of the system's resource consumption under load

and identification of potential performance bottlenecks, including monitoring aspects of Wazuh's internal components like OpenSearch is configured.

3.6 Research Quality and Validity

The quality of the solution is appraised by simulating various operator events on the test OLT that constitutes suspicious fraudulent activities. The detection and alerting capabilities of the solution is validated for each simulated event.

3.7 Ethical Considerations

The system is deployed and tested on an isolated network to avoid disruption of communication on live networks. The research strictly adheres to ethical guidelines to protect data confidentiality and privacy. All testing is performed on a dedicated test environment without involving real customer data.

The research respects the rights, beliefs, perceptions, and cultural heritage of individuals by ensuring no human subjects are involved. All findings are presented objectively, with due regard for the welfare of stakeholders.

The research complies with Strathmore University research ethics requirements including seeking ethical approval and also adherence to NACOSTI research regulations.

3.7.1 Fair Distribution of and Access to Benefits

To ensure fair access to the research benefits, the findings and the prototype framework can be made available to academia, industry stakeholders and the broader cybersecurity community. Additionally, open-source components such as Wazuh custom rules developed during this research may be shared publicly to benefit other researchers and ISPs facing similar GPON fraud risks.

Chapter 4: System Design and Architecture

4.1 Introduction

The chapter details the main features of the GPON fraud detection solution design architecture. The design process handles OLT events in real time for detecting suspicious activity that signals potential fraud elements. The solution's functional operation is achieved by this chapter providing insights about its high-level architecture and main components and use cases while maintaining operational scalability and responsiveness within an operational GPON environment.

4.2 System Architecture

The GPON Fraud Detection solution comprises several modules working together to enable real-time detection of suspicious activities on OLT devices. Figure 4.1 shows the high-level layout and the core components of the solution.

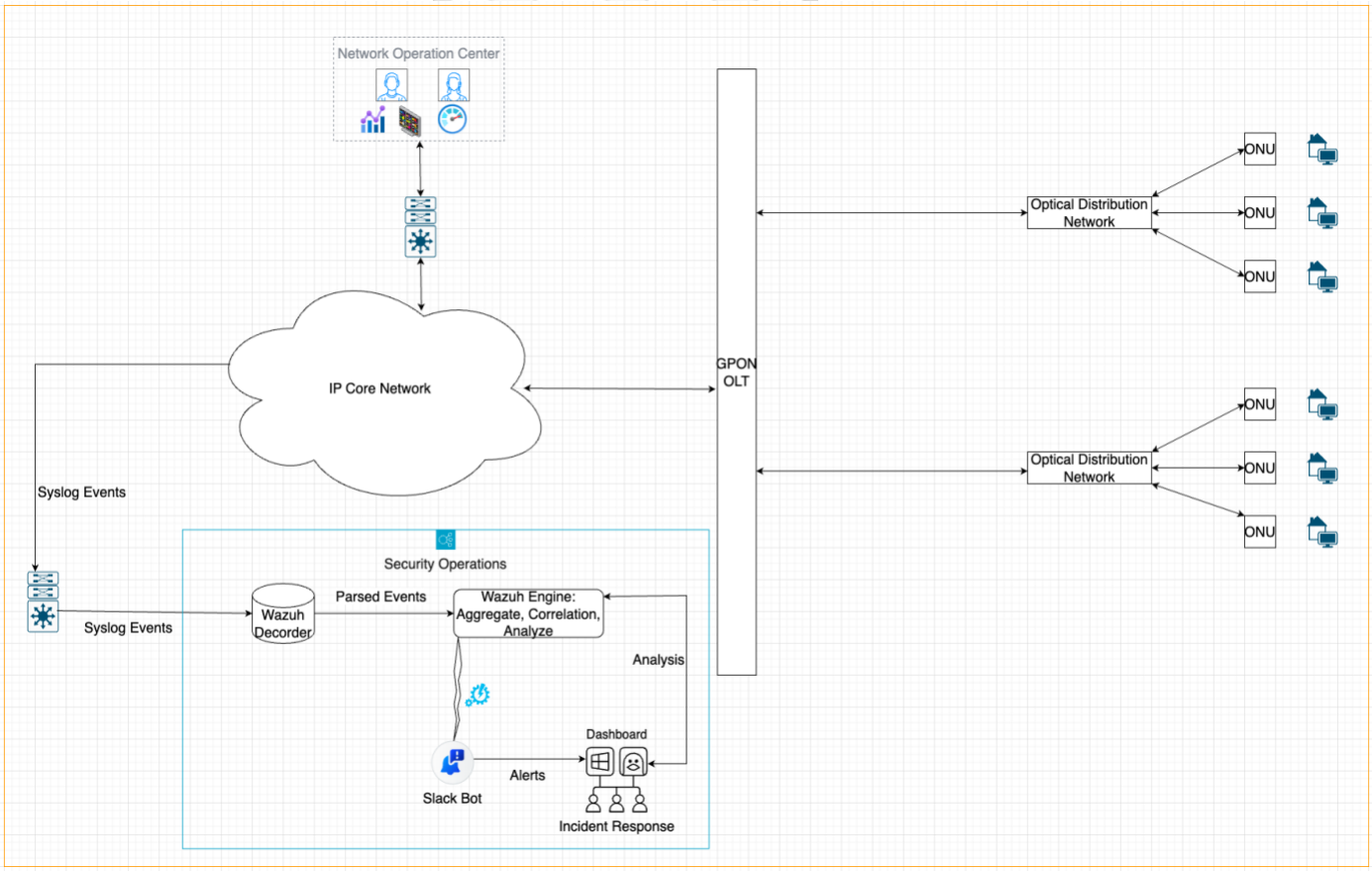


Figure 4.1: GPON Fraud Solution High Level Architecture

4.2.1 Custom Wazuh Decoders for OLT Event Parsing

The foundation of this framework is the deployment of custom Wazuh decoders tailored to parse specific fields from OLT event logs. Wazuh, a widely used open-source security platform offers customizable decoders that can be configured to extract key data from log entries. For GPON security, custom decoders are designed to parse and interpret events indicative of suspicious activity.[2]

The customized decoders focus on critical event types from the OLT. Each of these event logs contains specific information related to GPON operations and can reveal signs of potential security breaches. For instance, entries in the log can capture unauthorized configuration commands. By isolating these events, the decoders filter out routine log data ensuring that only potentially harmful activity is escalated for further analysis. By parsing and interpreting OLT events, custom Wazuh decoders create a streamlined approach for monitoring GPON activities and flagging high-risk incidents. This real-time data extraction enhances visibility into network behavior thus enabling administrators to detect and respond to suspicious activities quickly.

4.2.2 Centralized Wazuh Server for Detection, Analysis and Visualization

The Wazuh server acts as the central hub within this framework, aggregating and analyzing log data collected from custom decoders. By centralizing data collection, the Wazuh server allows for comprehensive monitoring, event correlation and security analysis, providing actionable insights into GPON's operational security.[3]

Aggregated Detection and Incident Analysis: The Wazuh server collects parsed log data from OLTs across the GPON network, enabling real-time detection of anomalies and high-risk activities. Events parsed by Wazuh decoders such as suspicious ONU registrations, unauthorized bandwidth adjustments and configuration changes are sent to the server for immediate analysis. The Wazuh server assesses each flagged event against predefined security thresholds, ensuring that any activity meeting critical criteria triggers an alert. By maintaining a centralized records of

[2] https://documentation.wazuh.com/current/user-manual/ruleset/decoders/custom.html
[3] https://documentation.wazuh.com/current/user-manual/manager/index.html

parsed log data, the server enables in-depth analysis of individual incidents in helping analysts understand the context and scope of each security event.

Enhanced Event Correlation: The server's ability to correlate events across multiple OLTs enhances situational awareness, allowing analysts to identify potential coordinated attacks or widespread anomalies. The Wazuh server's correlation capabilities enable analysts to distinguish between isolated anomalies and systematic threats, supporting a more informed response to security incidents.

Visualization for Improved Situational Awareness: The Wazuh server includes visualization tools that display security metrics and event patterns in real time, providing analysts with a graphical overview of network health and activity. Dashboards can show metrics such as the frequency of rogue ONU registration attempts, the volume of suspicious bandwidth allocation adjustments, or the distribution of configuration changes. By visualizing these metrics, analysts gain a clearer understanding of network activity trends, enabling proactive identification of emerging security risks.

The centralized Wazuh server's integration of detection, correlation and visualization tools offers a holistic approach to monitoring GPON security. By aggregating data from across the network and presenting it in an accessible format, the server allows for efficient threat detection and enhanced incident response.

4.2.3 Slack Bot Integration for Real-Time Alerting

Slack bot integration with the Wazuh server facilitates rapid communication of security events ensuring that incident response teams are immediately informed of potential threats. Using Slack's Webhook API, the bot delivers real-time alerts to designated Slack channels whenever the Wazuh server detects a high-risk event allowing teams to respond without delay.[4]

Automated Alert Delivery: The Slack bot automatically sends alerts to incident response channels whenever a critical event is detected by the Wazuh server. These alerts include essential information, such as the type of event, timestamp and affected OLT or ONU. For example, if the Wazuh server flags misuse of service account attempt, the bot generates an alert with details

[4] https://api.Slack.com/messaging/webhooks

necessary for immediate investigation. Automated alerting reduces response time thereby eliminating the need for manual log monitoring and allowing response teams to act swiftly.

Prioritization and Escalation of High-Severity Events: The Slack bot can be configured to prioritize alerts based on severity levels, ensuring that high-impact incidents receive immediate attention. This prioritization allows incident response teams to focus resources on the most pressing threats, facilitating an organized and efficient response to potential breaches.

Centralized Communication and Documentation: Slack channels provide a collaborative platform for incident response teams, enabling them to communicate, coordinate and document response actions in real time. By centralizing communication within Slack, teams can discuss the severity of each alert, share investigative findings and decide on appropriate responses. This centralized communication also serves as a historical record of each incident, supporting post-incident analysis and allowing teams to refine response protocols based on documented findings.

By integrating Slack for real-time alerting, this framework enhances response efficiency, ensuring that potential threats are communicated to the appropriate teams as they arise. The Slack bot's prioritization and documentation features further support a structured approach to incident management, enabling GPON networks to maintain a high level of operational security.

4.3 Use Case Modelling

The combined cases (use case and Misuse cases) of the GPON fraud detection system are shown on Figure 4.2. The actors are malicious operators and security or fraud analysts.

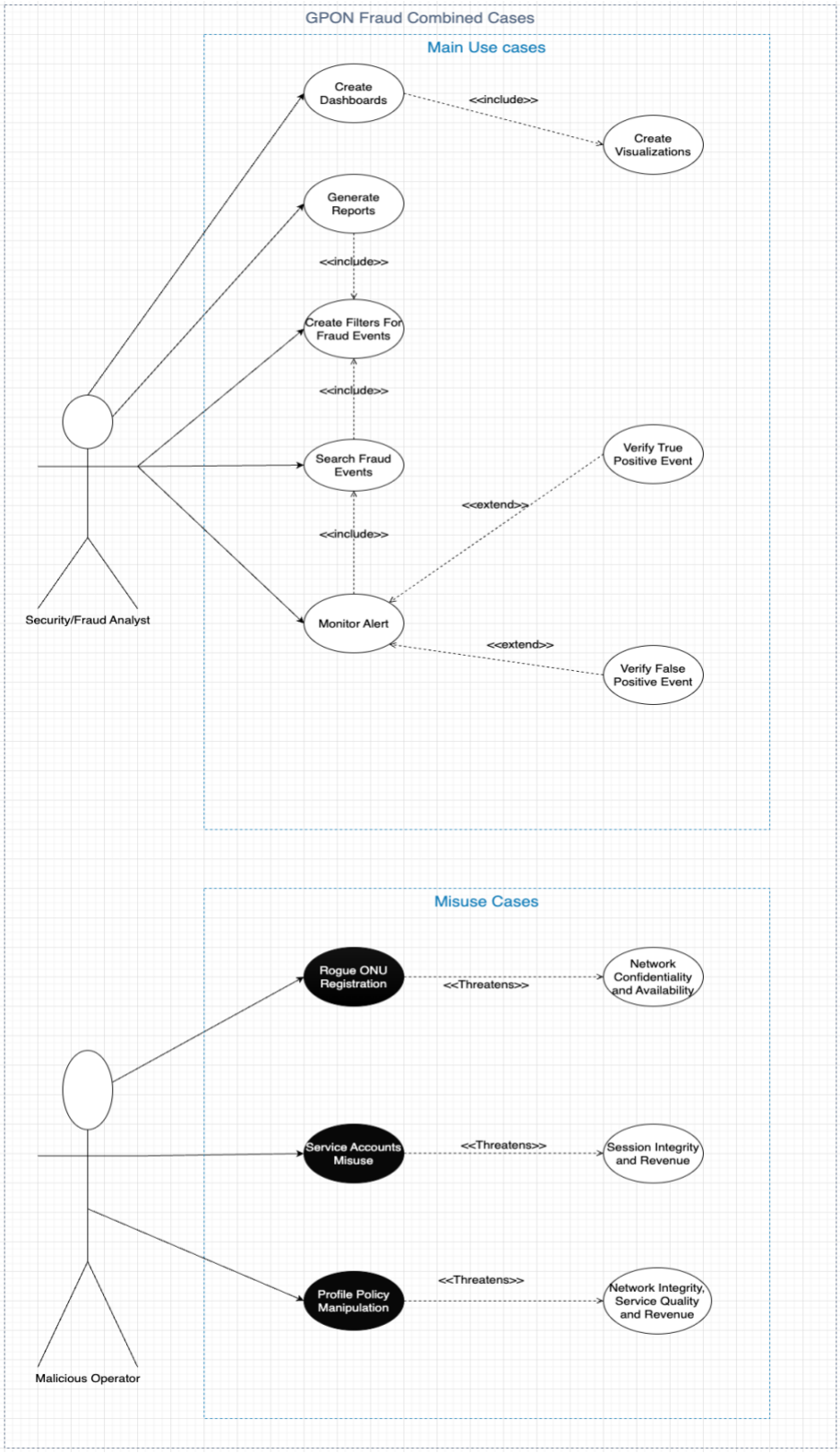


Figure 4.2: GPON Fraud Solution Combined Cases

4.3.1 Use Case 1: Search Events

Table 4.1 shows how the fraud analyst can search the system for events of related to fraudulent operations.

Table 4.1: Search Events Use Case

Use Case	Search Events
Scenario	Done using a web browser on Wazuh Dashboard
Description	The security/fraud analyst creates a search criterion based on time ranges, IP addresses or other strings that can identify events. The system then displays matching event logs.
Actors	Security/Fraud Analyst
Preconditions	1. The system must have received and indexed events. 2. The user has appropriate permissions to perform searches.
Post-conditions	1. Results of the search are displayed to the user. 2. The user can refine the search further if needed.
Flow of Events (Steps)	Actor 1. Enters search criteria (e.g., date range, IP, username). System 1. Retrieves all matching events from the indexed database. 2. Displays the results through the web interface.

4.3.2 Use Case 2: Create Filters

Table 4.2 depicts how an analyst can create filters to search and easily reuse common searching criteria.

Table 4.2: Create Filters Use Case

Use Case	Create Filters
Scenario	Done using a web browser on Wazuh Dashboard
Description	The security/fraud analyst searches and saves frequently used search criteria as filters for quick reuse.
Actors	Security/Fraud Analyst
Preconditions	1. The user has successfully performed a search or knows valid criteria. 2. The user has permission to save filters.
Post-conditions	1. The saved filter is available for future searches. 2. The user can see the newly created filter in a list of saved filters.
Flow of Events (Steps)	**Actor** 1. Creates or refines a search criterion. 2. Clicks “Save Filter” and provides a filter name. **System** 1. Validates the search criterion and saves it as a named filter. 2. Confirms filter creation to the user.

4.3.3 Use Case 3: Generate Fraud Reports

Table 4.3 describes how an analyst generates reports summarizing potential fraud indicators from the event data.

Table 4.3: Generate Fraud Report Use Case

Use Case	Generate Fraud Reports
Scenario	Done using a web browser on Wazuh Dashboard
Description	The analyst compiles suspicious events, anomalies, or flagged incidents into a structured report.
Actors	Security/Fraud Analyst

Use Case	Generate Fraud Reports
Preconditions	1. The system has collected and indexed event data. 2. The user has permission to generate and view reports.
Post-conditions	1. A report (e.g., PDF, HTML) is generated and available for download or viewing. 2. The report can be archived or shared.
Flow of Events (Steps)	**Actor** 1. Selects the "Generate Report" function. 2. Specifies a time range or filter criteria. **System** 1. Aggregates event data matching the criteria. 2. Formats and generates the report. 3. Displays or offers the file to the user.

4.3.4 Use Case 4: Create Dashboards and Visualizations

Table 4.4 covers how the analyst creates dashboards and visualization charts (e.g., bar charts, pie charts) to monitor trends in near real-time.

Table 4.4: Create Dashboards and Visualization

Use Case	Create Visualizations
Scenario	Done via a web browser on Wazuh Dashboard
Description	The analyst builds interactive charts and dashboards from event data to track suspicious activities and trends.
Actors	Security/Fraud Analyst
Preconditions	1. The system contains indexed event data. 2. The user has the necessary privileges to create and save dashboards.
Post-conditions	1. A new visualization or dashboard is created. 2. The user can share or export the visualization

Use Case	Create Visualizations
Flow of Events (Steps)	**Actor** 1. Chooses data fields (e.g., event type, timestamp). 2. Selects visualization type (bar chart, line chart, etc.). 3. Clicks “Save.” **System** 1. Builds the requested visualization. 2. Displays it to the user in a dashboard layout.

4.3.5 Use Case 5: Monitor Alerts

Table 4.5 explains how the analyst views and responds to triggered alerts in the system (e.g., suspicious policy change events, rogue ONU events).

Table 4.5: Monitor Alerts Use Case

Use Case	Monitor Alerts
Scenario	Done via a web interface on Wazuh Dashboard or messaging integration on Slack monitoring channel
Description	The user is notified when certain high-risk events occur and can review these alerts in an alerts console.
Actors	Security/Fraud Analyst
Preconditions	1. Alert rules or filters have been configured. 2. The system is actively collecting and evaluating events.
Post-conditions	1. Alerts are displayed in the user interface. 2. The user can acknowledge or investigate each alert.
Flow of Events (Steps)	**Actor** 1. Opens the alerts dashboard or receives a notification. 2. Clicks on an alert to view details. **System** 1. Retrieves alert data (time, severity, event details). 2. Displays the full alert information.

4.3.6 Misuse Case 1: Rogue ONU Registration

Table 4.6 misuse case arises when an attacker or insider adds an unauthorized Optical Network Unit to the GPON, allowing data interception or unauthorized resource use.

Table 4.6: Rogue ONU Registration Misuse Case

Misuse Case	Rogue ONU Registration
Threatens	Network confidentiality and availability
Description	A malicious operator/attacker registers the serial number of a rogue ONU, potentially intercepting traffic and causing service issues.
Actors (Misuser)	Malicious Operator/Attacker
Preconditions	1. The attacker has knowledge of a valid ONU identifier or has insider access to the OLT. 2. The attacker has access to the OLT
Post-conditions	1. Interception or eavesdropping on downstream traffic. 2. Disruption or bandwidth theft affecting legitimate ONUs.
Flow of Events (Steps)	Malicious Operator / Attacker 1. Acquires valid ONU credentials or spoofs a serial number. 2. Initiates registration of the rogue ONU. System 1. Accepts and configures the ONU, assigning resources. 2. Logs the registration event but may not flag it if lacking robust detection.

4.3.7 Misuse Case 2: PPPoE Service Account Misuse

Table 4.7 misuse case occurs when an attacker exploits or steals valid PPPoE credentials to gain unauthorized network access or commit fraud.

Table 4.7: Service Account Misuse Case

Misuse Case	PPPoE Service Account Misuse
Threatens	Authentication framework, session integrity and Revenue
Description	Malicious Operators leverage zero rated PPPoE credentials meant for service testing purpose for zero rated access
Actors (Misuser)	Malicious Operator
Preconditions	1. Attacker obtains valid PPPoE username/password 2. BRAS/AAA servers accept PPPoE sessions without additional multi-factor checks.
Post-conditions	1. Unauthorized access to network resources. 2. Potential billing fraud or data exfiltration.
Flow of Events (Steps)	**Malicious Operator / Attacker** 1. Attempts PPPoE login using compromised credentials. 2. Establishes a session, bypassing legitimate user restrictions. **System** 1. Authenticates the PPPoE request if the credentials are valid. 2. Grants network access

4.3.8 Misuse Case 3: Policy Manipulation

Table 4.8 misuse case occurs when a malicious operator or attacker alters GPON service or configuration policies for fraudulent purposes.

Table 4.8: Policy Manipulation Misuse Case

Misuse Case	Policy Manipulation
Threatens	Network integrity and Quality of Service
Description	An operator/attacker with privileged or compromised credentials modifies critical GPON policies (e.g., bandwidth allocations, service profiles) to gain unauthorized benefits or degrade legitimate services.

Misuse Case	Policy Manipulation
Actors (Misuser)	Malicious Operator
Preconditions	1. Malicious operator has sufficient access rights or has exploited a vulnerability. 2. GPON system allows remote or local configuration changes.
Post-conditions	1. Service disruptions or unauthorized upgrades/downgrades to subscriber services. 2. Potential billing or revenue impact.
Flow of Events (Steps)	**Malicious Operator** 1. Logs into the OLT or management system with stolen or misused credentials. 2. Navigates to the policy settings (e.g., bandwidth profiles). 3. Changes the policies to achieve malicious goals (free upgrades, denial of service, etc.). **System** 1. Saves or applies the new policies, distributing them to ONUs. 2. Reflects these changes in subsequent system logs.

4.4 GPON Fraud Sequence Diagram

Figure 4.3 shows a sequence diagram with the processes that occur from OLT events ingestion to triggering of an alert and investigation of the suspicious events in the GPON fraud system.

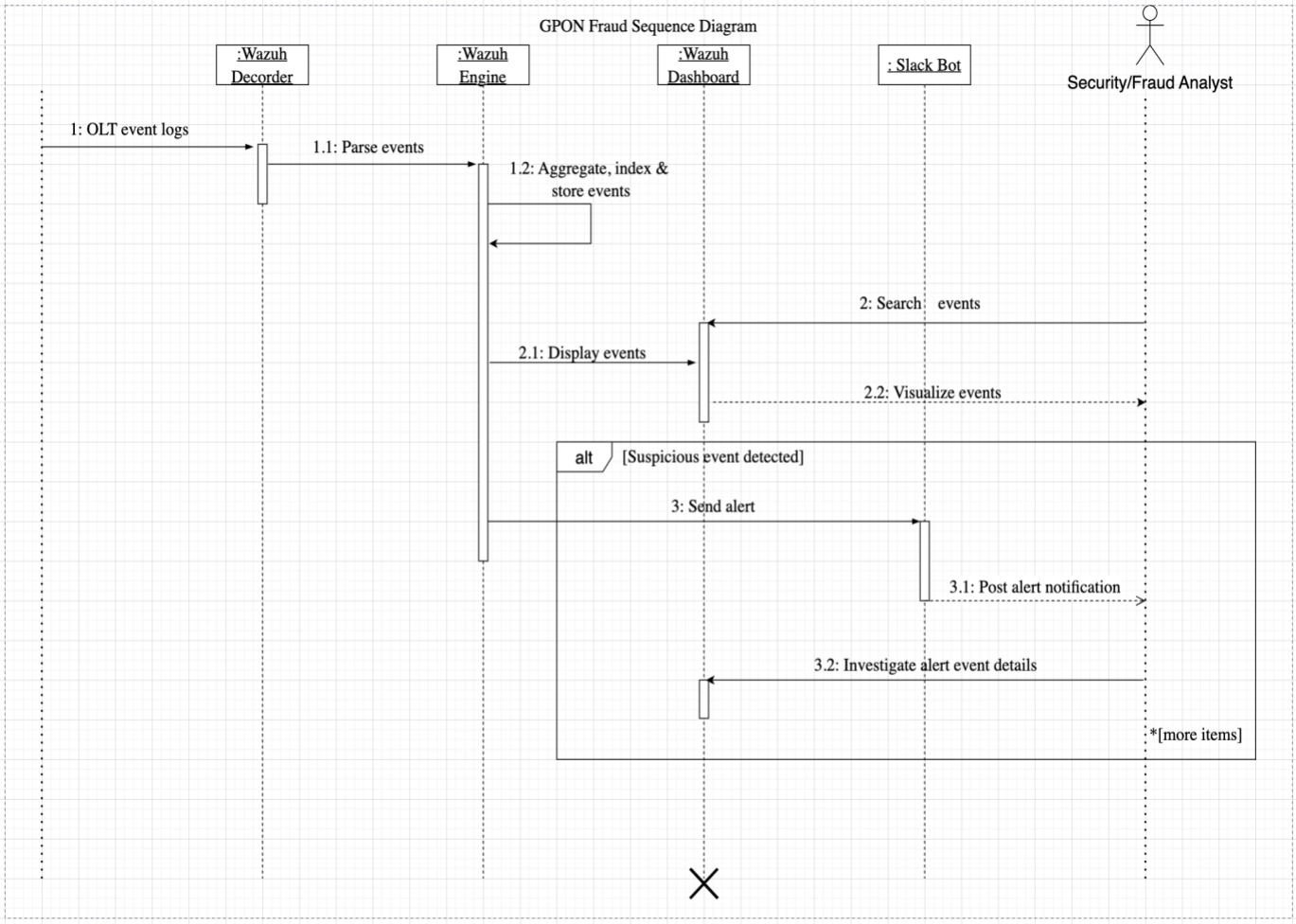


Figure 4.3: GPON Fraud Sequence Diagram

The following are sequence of events in the GPON Fraud System:

4.4.1 Step 1: OLT Event Log Ingestion

The OLT generates event logs related to network activities. These logs are sent to the Wazuh Decoder.

4.4.2 Step 1.1: Event Parsing

The Wazuh Decoder processes the raw event logs and parses them based on the predefined decoders. The parsed events are forwarded to the Wazuh Engine.

4.4.3 Step 1.2: Event Aggregation, Indexing and Storage

The Wazuh Engine composed of Filebeat, Indexer and Manager aggregates and indexes the received events. The processed events are stored and made available for search and visualization.

4.4.4 Step 2: Event Search

The Security/Fraud Analyst can search events through the Wazuh Dashboard.

4.4.5 Step 2.1: Event Display

The Wazuh Dashboard fetches the events from Wazuh Engine.

4.4.6 Step 2.2: Visualize Events

The Security/Fraud Analyst is able to view the visualized events displayed from Wazuh Engine using the Wazuh Dashboard.

4.4.7 Step 3: Detection and Alert Trigger

If a suspicious fraudulent event is detected, the system triggers an alert. The Wazuh Engine sends an alert to the Slack Bot.

4.4.8 Step 3.1: Alert Notification

The Slack Bot posts a notification about the detected suspicious event on the Slack monitoring channel. The Security/Fraud Analyst is informed via the Slack notification.

4.4.9 Step 3.2: Alert Investigation

The Security/Fraud Analyst accesses the Wazuh Dashboard and investigates the alert details. Further actions may be taken based on the findings.

For every alert triggered on the system. The sequence of events repeats in a loop from Step 3 to Step 3.2 until all alerts are investigated. The Security or Fraud analyst upon completion of investigation logouts of the Wazuh Dashboard and the sequence of events terminates.

Chapter 5: System Implementation and Testing

5.1 Introduction

This chapter discusses the implementation and testing of the GPON Fraud Detection System designed to ingest, analyze, visualize and provide near real-time alerts on fraudulent activities detected from OLT operator events. The chapter describes system specifications, configuration steps, key features and comprehensive tests conducted to ensure functionality, reliability and effectiveness in detecting GPON-related fraud.

5.2 System Specification

The GPON Fraud Detection Platform is implemented on a testbed with the following key components:

a. ZTE OLT version C300

b. Wazuh Sever

   i. Ubuntu Server 24.04.2 LTS

   ii. 32 GB RAM

   iii. 500 GB Disk

   iv. Wazuh Indexer version 4.11.0

   v. Wazuh Manager version 4.11.0

   vi. Filebeat version 7.10.2

   vii. Wazuh Dashboard version 4.11.0

c. Slack Bot

d. Telegraf version 1.34.1 and InfluxDB version 2.7.11

5.3 System Implementation and Testing

5.3.1 OLT Event Collection Configuration

The event collection is configured on the ZTE OLT to forward all event activities to the Wazuh server running on Ubuntu. OLT Syslog forwarding is enabled via command-line interface (CLI) as shown on Figure 5.1:

```
TEST_OLT_C300_248.12(config)#logging cmdlog enable
TEST_OLT_C300_248.12(config)#$t 514 lport 514 cmdlog facility local0
TEST_OLT_C300_248.12(config)#syslog-server host enable 10.15.10.5 fport 514
```

Figure 5.1: OLT Syslog Configuration

The logs are transmitted using UDP port 514.

5.3.2 Event Ingestion, Parsing, Storage and Visualization

The individual components of the event analysis were installed in Ubuntu 24.04.2 LTS operating system, see Appendix B. Since each component is an independent component, the configurations were made to allow for communication between them to be possible through specific ports with necessary configuration parameters:

i. Wazuh manager was configured to receive syslog events from the test OLT on port 514 udp.

ii. Custom Wazuh decoders were developed to parse OLT command logs.

iii. Filebeat was configured to send events and alerts to the Wazuh indexer for indexing and storage

iv. Wazuh dashboard was configured to be accessed through port 443.

5.3.2.1 Wazuh Ingestion

```
<remote>
  <connection>syslog</connection>
  <port>514</port>
  <protocol>udp</protocol>
  <allowed-ips>192.168.248.12</allowed-ips>
  <local_ip>10.15.10.5</local_ip>
</remote>
```

This configuration ensures that Wazuh receives events from the OLT (192.168.248.12) on port 514 using the UDP protocol. The allowed-ips field restricts access, meaning only the specified IP can receive the logs. local_ip specifies the network interface (10.15.10.5) from which logs will be sent.

5.3.2.2 Custom Wazuh Decoders

Custom Wazuh decoders were developed for detecting GPON fraud events. These decoders analyze OLT command logs, extracting key fields using PCRE2 regular expressions. They are designed to identify distinct patterns corresponding to the misuse cases identified and designed in chapter 4. The following are the developed sample decoders, PPPoE username, ONU registrations and user-VLAN policy configuration events.

```
<decoder name="olt-command-log-pppoe">
        <program_name>command-log</program_name>
        <prematch type="pcre2">^.*?\d*\s+\S+\s+\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s+pppoe\s+\d+\s+nat enable user
\S+\s+password\s+.*</prematch>
   <regex type="pcre2">.*?(ssh\d*|vty\d*)\s+(\S+)\s+(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s+pppoe\s+\d+\s+nat enable user
(\S+)\s+password\s+.*</regex>
   <order>session_type, srcuser, srcip, pppoe_username</order>
</decoder>
```

This decoder targets log entries that indicate configuration PPPoE account on a user interface connected to an ONU. It is used to extract details like the session type, source user, source IP and PPPoE username configured.

i. program_name: Specifies that the logs originate from the command-log syslog program.

ii. prematch: Uses a PCRE2 pattern to quickly filter relevant logs that include an IP address, the keyword pppoe and the text nat enable user. This reduces unnecessary processing.

iii. regex: Applies a detailed pattern to capture specific fields:

   a. Session type (e.g., ssh or vty with an optional number).

   b. Source user (identifier for the user initiating the command).

   c. Source IP (matches a standard IPv4 address).

   d. PPPoE username (extracts the configure username).

iv. order: Specifies the order in which captured fields are returned: session_type, srcuser, srcip, pppoe_username.

```
<decoder name="olt-command-log-onu-registration">
    <program_name>command-log</program_name>
    <prematch type="pcre2">^.*?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s+onu\s+\d+\stype\s\S+\s+sn\s+\S+</prematch>
  <regex
type="pcre2">^.*?(ssh\d*|vty\d*)\s+(\S+)\s+(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s+onu\s+\d+\stype\s(\S+)\s+sn\s+(\S+)</regex>
  <order>session_type, srcuser, srcip, onu_model, onu_serial_number</order>
</decoder>
```

This decoder is aimed at capturing events related to ONU registration. It extracts details such as session type, source user, source IP, ONU model and the ONU serial number.

i. program_name: Indicates the log source is command-log.

ii. prematch: Filters for log lines containing an IP address, the keyword onu and a serial number (sn).

iii. regex: Breaks down the log into:

   a. Session type (identifying whether the connection is via ssh or vty).

   b. Source user.

   c. Source IP.

   d. ONU model.

   e. ONU serial number.

iv. order: Determines the output order: session_type, srcuser, srcip, onu_model, onu_serial_number.

```
<decoder name="olt-command-log-bandwidth-abuse">
    <program_name>command-log</program_name>
    <prematch
type="pcre2">.*?\d*\s+\S+\s+\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s+profile\s+tcont\s+\S+\s+type\s+\d+\s+\S+\s+\S+.*</prematch
>
    <regex
type="pcre2">.*?(ssh\d*|vty\d*)\s+(\S+)\s+(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s+profile\s+(tcont)\s+(\S+)\s+type\s+(\d+)\s+(\S
+)\s+(\S+).*</regex>
  <order>session_type, srcuser, srcip, bandwidth_profile, bandwidth_profile_name, bandwidth_type, bandwidth_type_name,
bandwidth_QOS</order>
</decoder>
```

This decoder identifies potential bandwidth profile abuse by parsing logs where profile, tcont and type are mentioned. It focuses on extracting session_type, srcuser, srcip, bandwidth_profile, bandwidth_profile_name, bandwidth_type, bandwidth_type_name, bandwidth_QOS from the logs.

i. program_name: Again, the log entries come from command-log.

ii. prematch: Filters entries that include an IP address, followed by keywords like profile, tcont and type . This step ensures that only logs with tcont profile references are processed.

iii. regex: Captures the following fields:

   a. Session type (either ssh or vty variants).

   b. Source user.

   c. Source IP.

   d. Bandwidth Profile and Bandwidth Profile Name

   e. Bandwidth Type, and Bandwidth Type Name,

   f. Bandwidth Quality of Service

iv. order: Sets the extraction order as session_type, srcuser, srcip, user_vlan_id.

These custom decoders enhance Wazuh's ability to detect and analyze potential fraud events in GPON environments enabling targeted monitoring and timely responses to security incidents. The decoders can be customized to meet different GPON Fraud scenarios for different service providers.

5.3.2.3 Wazuh Indexer Configuration

This configuration file establishes network settings, cluster parameters, storage paths and robust security settings using SSL for both HTTP and transport layers.

```
network.host: "10.15.10.5"
node.name: "node-1"
```

This setting binds the indexer to the IP address 10.15.10.5, ensuring that the service is reachable

on this network interface. The node is given a unique identifier (node-1) which is used within the cluster to distinguish it from other nodes.

```
cluster.initial_master_nodes:
 - "node-1"
cluster.name: "wazuh-cluster"
```

This setting lists the initial master-eligible nodes required to bootstrap the cluster. In this example only node-1 is active but there is a possibility of additional nodes, node-2 and node-3 or more for a multi-node setup. The cluster is named "wazuh-cluster", grouping all related nodes under a single cluster identity.

```
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer
```

Specifies where the indexer stores its data files. In this case, all persistent data is kept in /var/lib/wazuh-indexer. Logs generated by the indexer are written to /var/log/wazuh-indexer, facilitating monitoring and troubleshooting.

```
plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.http.enabled: true
```

The security section configures SSL/TLS settings for both HTTP communications (client-facing API calls) and internal transport communications (between cluster nodes).

PEM Certificate, Key, and Trusted CA:

i. The HTTP interface uses a certificate (indexer.pem) and a key (indexer-key.pem) to establish secure connections.

ii. The trusted CA certificate (root-ca.pem) is used to validate incoming HTTPS connections.

The HTTP SSL layer is enabled, ensuring that all HTTP communication is encrypted.

```
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false
```

Similar to the HTTP settings, the transport layer (used for inter-node communication) is secured using the same certificate, key and trusted CA.

Hostname verification is disabled (enforce_hostname_verification: false) and the hostname resolution is not enforced (resolve_hostname: false). These settings may simplify configuration in environments with dynamic or private IPs but should be evaluated carefully in production to ensure they meet your security requirements.

5.3.2.4 Filebeat Configuration

This Filebeat configuration file is tailored for this deployment. It specifies secure output settings to Elasticsearch, activates the Wazuh module for processing alerts and sets up logging and security policies. Each section is explained in detail below.

```
output.elasticsearch:
  hosts: ["10.15.10.5:9200"]
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/filebeat.pem"
  ssl.key: "/etc/filebeat/certs/filebeat-key.pem"
```

Filebeat is set to forward events to an Elasticsearch instance hosted at 10.15.10.5 on port 9200, using the secure HTTPS protocol.

The configuration uses environment variables for the username and password (${username} and ${password}) to provide credentials hence ensuring that sensitive information isn't hard-coded.

The SSL options provide a secure connection:

i. ssl.certificate_authorities specifies the root CA for certificate validation.

ii. ssl.certificate and ssl.key provide the client certificate and key for mutual TLS authentication.

```
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false
```

These settings enable a JSON index template that Filebeat will install in the manager. The template file is located at /etc/filebeat/wazuh-template.json. The template is named wazuh, ensuring that indices created for Wazuh events follow the defined structure.

Index Lifecycle Management (ILM) disabled (setup.ilm.enabled: false), but setup.ilm.overwrite: true ensures that if ILM were used it would update any existing policy with the new configuration.

```
#Filebeat HTTP Endpoint for Metrics

http.enabled: true

http.host: 10.15.10.5

http.port: 5066
```

Filebeat HTTP Endpoint is enabled to expose Filebeat metrics for monitoring and debugging on 10.15.10.5 listening on Port: 5066.

```
filebeat.modules:
 - module: wazuh
   alerts:
```

```
    enabled: true
  archives:
    enabled: false
```

The Wazuh module is enabled to process and structure alert data coming from Wazuh. Alerts are actively collected (enabled: true). Archive processing is disabled (enabled: false) focusing the module on real-time alert data.

```
logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
  keepfiles: 7
  permissions: 0644

logging.metrics.enabled: false
```

Logging is set to the info level, ensuring moderate detail about Filebeat's operations. Logs are written to files:

i. Stored in /var/log/filebeat

ii. Log files are named filebeat

Up to 7 rotated log files are kept with file permissions set to 0644. Collection of logging metrics is disabled, simplifying the logging output.

```
seccomp:
  default_action: allow
  syscalls:
  - action: allow
    names:
    - rseq
```

This section defines security policies for system calls. The default action is to allow system calls. The rseq syscall is explicitly allowed which may be required by Filebeat or its modules for performance optimizations or other low-level operations.

5.3.2.5 Wazuh Dashboard Configuration

```
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://10.15.10.5:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersAllowlist: ["securitytenant","Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wz-home
```


This configuration file establishes a secure, robust and user-friendly setup for the Wazuh dashboard. The dashboard listens on all interfaces over HTTPS on port 443. It securely connects to an OpenSearch instance at https://10.15.10.5:9200. SSL is enabled with specified key and certificate files and the system allows only specific headers for requests. Multi-tenancy is disabled, and access is restricted to read-only roles as needed. The default landing page is configured to /app/wz-home, streamlining the user experience.

This configuration ensures that the Wazuh dashboard can securely and effectively visualize security data, while maintaining a high level of integrity and access control.

5.3.3 Event Alerting

After the event ingestion and custom parsing of OLT events using custom decoders, the events are indexed and stored using Wazuh indexer. The following details how the events are correlated and events that meet certain criteria trigger alerts. Alerts are forwarded to a Slack channel using a Slack bot which utilizes an incoming webhook. Fraud or security analysts get the notification via Slack and access the platform to analyze and respond accordingly.

5.3.3.1 Wazuh Alert Rules and Slack Integration

Wazuh alert rules were designed to detect potential fraud events on OLT devices. These rules group alerts by event type such as PPPoE service account activity, ONU registration anomalies and user-VLAN policy abuse and leverage custom decoders and lookup lists to trigger high priority alerts when suspicious activity is detected.

```
<group name="olt,pppoe,fraud">
  <rule id="100003" level="10">
    <decoded_as>olt-command-log-pppoe</decoded_as>
    <list field="pppoe_username" lookup="match_key">etc/lists/pppoe_service_accounts</list>
    <description>PPPoE Service Account "$(pppoe_username)" from watch list enabled from $(srcip) on $(hostname) via
$(session_type) by $(srcuser)</description>
    <mitre>
      <id>T1078</id>
      <id>T1555</id>
    </mitre>
  </rule>
</group>
```

i. Group and Rule ID: The rule belongs to the group olt,pppoe,fraud and uses the unique identifier 100003 with a severity level of 10.

ii. Decoded As: The rule is applied to events processed by the olt-command-log-pppoe decoder.

iii. List Matching: It uses a lookup list (from etc/lists/pppoe_service_accounts) to check if the extracted pppoe_username exists in a predefined watch list of restricted service accounts. If a match is found, it indicates that the PPPoE service account is being used in a context that warrants further investigation.

iv. Description: The alert description dynamically inserts the values extracted from the log such as the pppoe_username, source IP (srcip), hostname, session type (session_type) and source user (srcuser) to provide clear context for the alert.

v. MITRE ATT&CK IDs: The inclusion of MITRE IDs T1078 (valid accounts) and T1555 (credentials from password stores) provides additional context on the type of tactics or techniques that the alert might be associated with.

```
<group name="olt,onu,registration,fraud">
  <rule id="100004" level="10">
        <decoded_as>olt-command-log-onu-registration</decoded_as>
        <list field="onu_serial_number" lookup="not_match_key">etc/lists/authorized_onus</list>
    <description>Rogue ONU registration detected: Model $(onu_model), Serial Number $(onu_serial_number) from $(srcip) via
$(session_type) by $(srcuser) on $(hostname).</description>
    <mitre>
      <id>T1078</id>
      <id>T1555</id>
    </mitre>
  </rule>
</group>
```

i. Group and Rule ID: This rule is placed in the group olt,onu,registration,fraud with the ID 100004 and a level 10 severity.

ii. Decoded As: The rule applies to events decoded as olt-command-log-onu-registration.

iii. List Matching (Not Match): It verifies that the onu_serial_number does not match any value in the lookup list etc/lists/authorized_onus. A non-match indicates a potential rogue or unauthorized ONU registration.

iv. Description: The description incorporates dynamic values such as the ONU model, serial number, source IP, session type, source user and hostname, making it clear what constitutes suspicious behavior.

v. MITRE ATT&CK IDs: The rule references MITRE IDs T1078 and T1555 to provide insight into the techniques related to unauthorized access and credential usage.

```
<group name="olt,bandwidth,abuse,fraud">
  <rule id="100007" level="10">
        <decoded_as>olt-command-log-bandwidth-abuse</decoded_as>
    <list field="bandwith_profile_name" lookup="not_match_key">etc/lists/bandwith</list>
    <description>Bandwidth Profile manipulation detected: Profile $(bandwith_profile_name) type $(bandwith_profile_type)
QOS $(bandwidth_QOS) configured by $(srcuser) on $(hostname).</description>
    <mitre>
      <id>T1078</id>
      <id>T1555</id>
      <id>T1562.001</id>
    </mitre>
  </rule>
</group>
```

i. Group and Rule ID: This rule is within the group olt,bandwidth, abuse,fraud and carries the ID 100007 with a severity level of 10.

ii. Decoded As: The event is processed by the olt-command-log-bandwidth-abuse decoder.

iii. List Matching (Not Match): It verifies that the bandwidth_profile_name does not match any value in the lookup list etc/lists/bandwidth. A non-match indicates a bandwidth policy manipulation activity.

iv. Description: The alert description provides context by including details such as the bandwidth profile name, configured QOS, source IP, session type, source user and hostname.

v. MITRE ATT&CK IDs: In addition to T1078 and T1555, this rule also references T1562.001, which relates to the compromise of user data or configuration manipulation.

These Wazuh alert rules are designed to detect specific types of fraud and unauthorized activities related to GPON networks on OLT devices. Rules can be customized based on different decoders customized to meet different GPON fraud scenarios for different service providers.

Once alert rules are configured and alerts are triggered, they are forwarded to a Slack channel using a webhook URL, filtering alerts by specific rule IDs, alert level and groups.

```
<integration>
  <name>Slack</name>
  <hook_url>https://hooks.Slack.com/services/T08JE4ES1UJ/B08HXRG4BBR/ZXmECAREZfip6MwcicSgiLlK</hook_url>
  <alert_format>json</alert_format>
  <!-- Optional filters -->
  <rule_id>100003,100004,100006</rule_id>
  <level>10</level>
  <group>olt,pppoe,fraud,onu,registration,uservlan,abuse</group>
</integration>
```

i. Integration Name

<name>Slack</name>

This tag defines the name of the integration. In this case, it is set to "Slack," indicating that the alerts will be sent to Slack.

ii. Slack Webhook URL

<hook_url>

The hook_url contains the full Slack Incoming Webhook URL. This URL is used by Wazuh to send alert notifications directly into a Slack channel. It is essential that this URL remains confidential to prevent unauthorized usage.

iii. Alert Format

<alert_format>json</alert_format>

This setting specifies that the alerts sent to Slack will be formatted as JSON. JSON formatting allows for structured data, which can be parsed and displayed in a readable format within Slack.

iv. Optional Filters

<rule_id>100003,100004,100006</rule_id>

This filter limits the integration to only forward alerts that match the specified rule IDs. In this configuration, only alerts with IDs 100003, 100004 and 100006 will be sent to Slack.

<level>10</level>

The level filter ensures that only alerts with a severity level of 10 (or higher, if configured differently) are forwarded. This helps in reducing noise by focusing on high-priority alerts.

<group>olt,pppoe,fraud,onu,registration,uservlan,abuse</group>

The group filter further refines the alerts by targeting specific groups. In this case, alerts from groups related to OLT fraud events covering PPPoE, ONU registration and user-VLAN abuse are forwarded.

By setting up this integration, security teams can promptly receive and respond to potential fraud events in their GPON environments via Slack, improving situational awareness and incident response times.

5.3.4 Performance Monitoring

Telegraf is installed as an agent on the Ubuntu server to collect system metrics such as CPU, RAM, disk I/O and OpenSearch performance at regular intervals. These metrics are sent to InfluxDB for visualization. This setup allows for tracking the performance impact of log ingestion, analysis and alerting

5.3.4.1 InfluxDB Configuration

```
bolt-path = "/var/lib/influxdb/influxd.bolt"
engine-path = "/var/lib/influxdb/engine"
```

These paths are part of the InfluxDB configuration and specify where certain data files are stored:

i. bolt-path: This is the path to the BoltDB file, which InfluxDB uses to store metadata such as tokens, users, and organizations. In this case, it's located at /var/lib/influxdb/influxd.bolt.

ii. engine-path: This is the path to the storage engine files, where InfluxDB stores the actual time-series data. In this configuration, it's located at /var/lib/influxdb/engine.

5.3.4.2 Telegraf Configuration

```
[[outputs.influxdb_v2]]
  urls = ["http://10.15.10.5:8086"]
  token = "XXXXXXXXXXX”
  organization = "gpon-fraud-lab"
  bucket = "gponfraud"
```

InfluxDB Output Plugin:

URLs: Specifies the address of the InfluxDB instance where Telegraf will send the collected metrics.

Token: An authentication token used to securely connect to the InfluxDB instance.

Organization: The name of the organization in InfluxDB where the data will be stored.

Bucket: The specific bucket within the organization where the metrics will be saved.

```
[[inputs.procstat]]
 systemd_unit = "wazuh-manager.service"
 include_systemd_children = true


[[inputs.procstat]]
 systemd_unit = "filebeat.service"
 include_systemd_children = true
```

Procstat Input Plugin:

i. Systemd Unit: Identifies the systemd service (e.g., wazuh-manager.service and filebeat.service) for which Telegraf will collect process statistics.

ii. Include Systemd Children: When set to true, it includes statistics for child processes of the specified systemd service.

```
[[inputs.http]]
 urls = ["http://10.15.10.5:5066/stats"]
 method = "GET"
 data_format = "json_v2"
```

HTTP Input Plugin:

i. URLs: The endpoint(s) from which Telegraf will fetch data.

ii. Method: The HTTP method used to request data (in this case, GET).

iii. Data Format: Specifies the format of the data returned by the HTTP endpoint (e.g., json_v2).

```
[[inputs.elasticsearch]]
 servers = ["https://10.15.10.5:9200"]
 username = "admin"
 password = "XXXXX"
 tls_ca = "/etc/telegraf/root-ca.pem"
 insecure_skip_verify = true
 local = true
 cluster_health = false
 cluster_stats = false
 cluster_stats_only_from_master = true
 indices_include = ["_all"]
 indices_level = "shards"
```

Elasticsearch Input Plugin:

i. Servers: The address of the Elasticsearch server(s) from which Telegraf will collect metrics.

ii. Username and Password: Credentials for authenticating with the Elasticsearch server.

iii. TLS CA: Path to the Certificate Authority file for verifying the server's SSL certificate.

iv. Insecure Skip Verify: When set to true, it skips SSL certificate verification (not recommended for production).

v. Local: Indicates whether to collect metrics only from the local node.

vi. Cluster Health and Cluster Stats: Options to enable or disable collection of cluster health and statistics.

vii. Cluster Stats Only From Master: Collects cluster statistics only from the master node.

viii. Indices Include: Specifies which indices to include in the metrics collection.

ix. Indices Level: The level of detail for index metrics (e.g., shards).

5.3.5 System Features

Once the security teams receive the alert notifications via Slack, they will access the Wazuh Dashboard to analyze and verify the triggered alerts and respond accordingly.

Analysts can search for events related to an alert, create search filters, create visualization and dashboard and also create reports related to certain activities.

5.3.5.1 Event Searching

Analysts can access the platform using a browser, which will display the web user interface provided by the Wazuh dashboard. Figure 5.2 shows an example of a search query **"test***

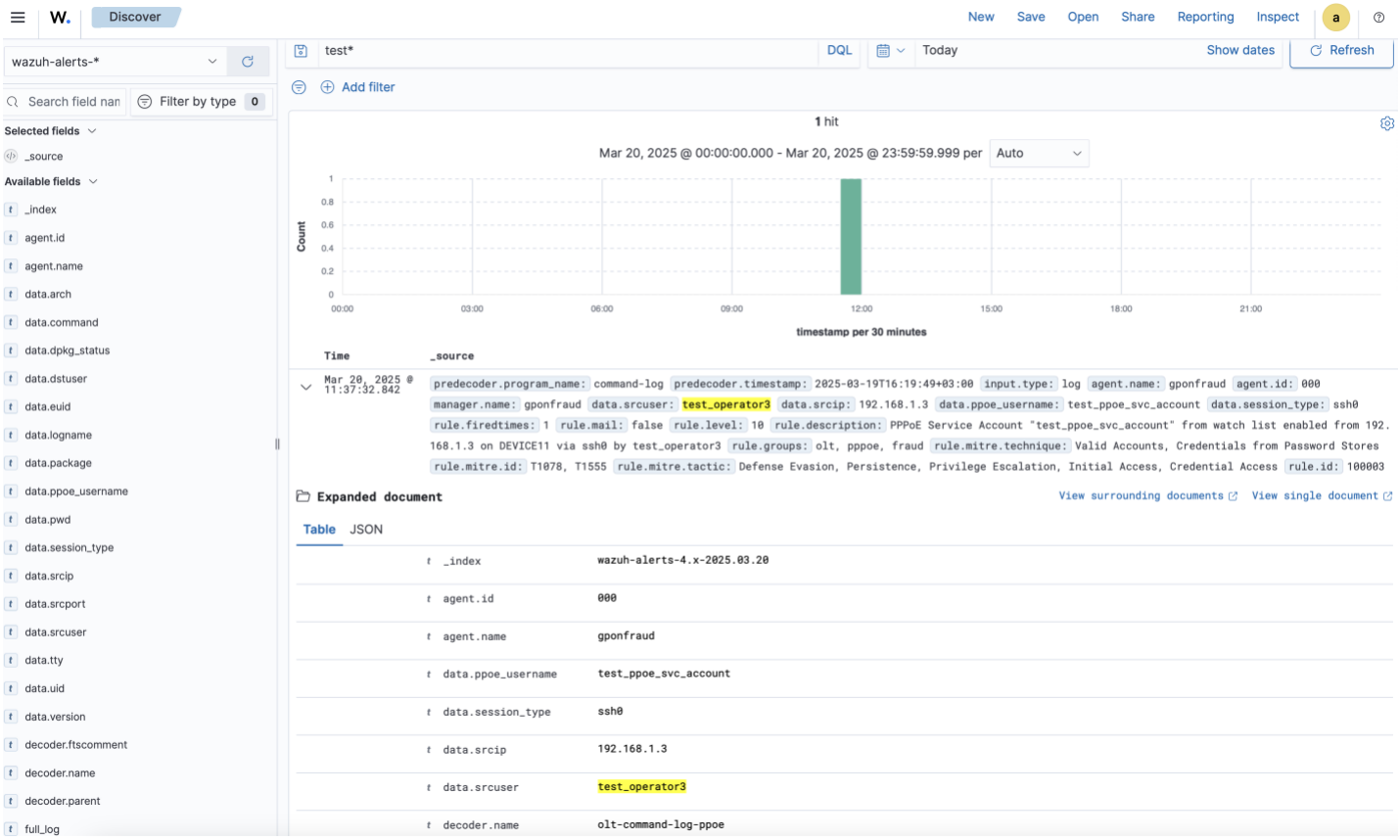


Figure 5.2: Event Search

5.3.5.2 Search Filters

The security/fraud analyst can search and save frequently used search criteria as filters for quick reuse. From Figure 5.3, an analyst can create a filter to match events associated with "olt-

command-log-pppoe" decoder. Search filters also facilitate creation of visualization based on search criteria.

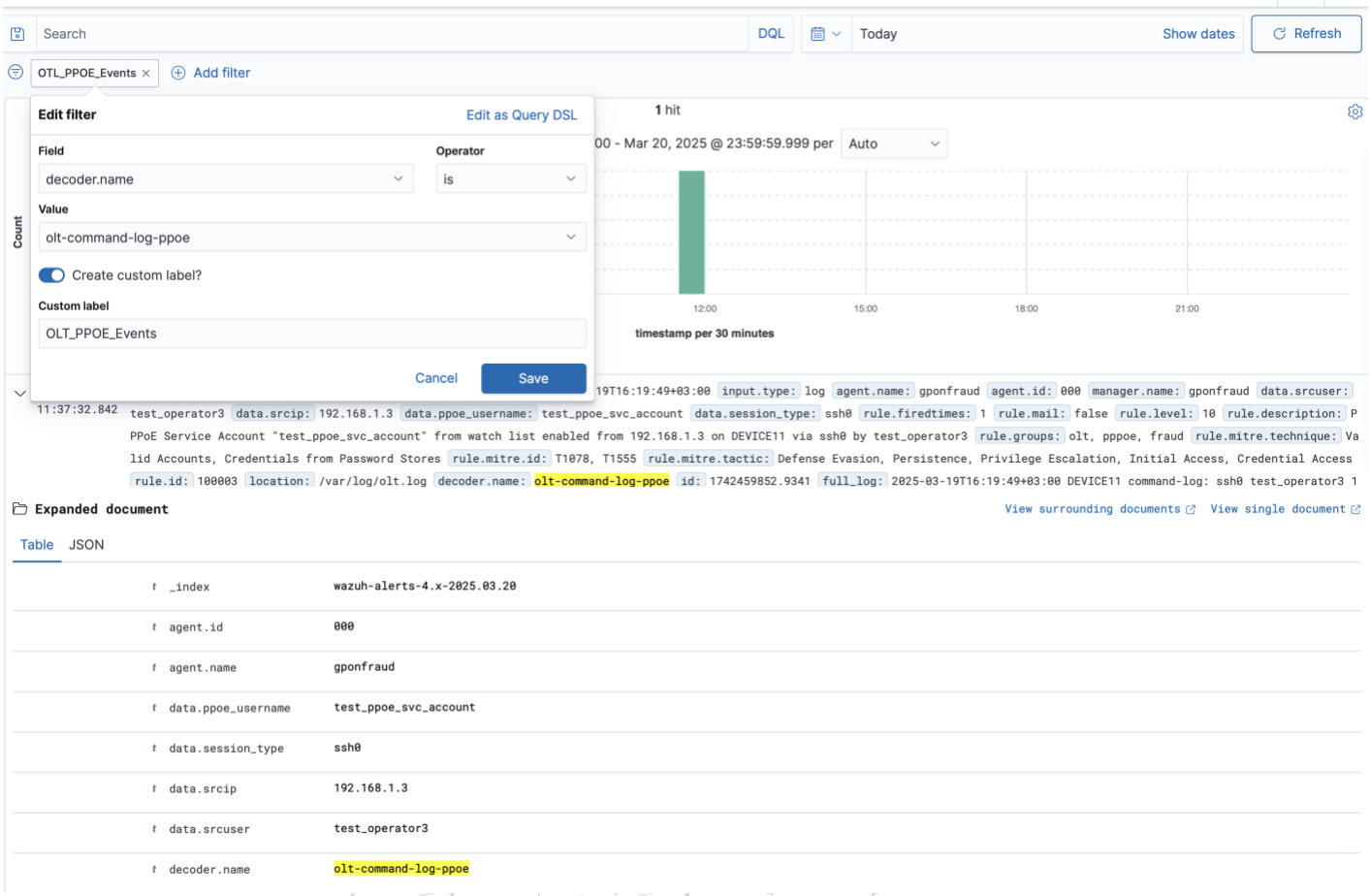


Figure 5.3: Seach Filter

5.3.5.3 Creating Visualizations and Dashboards

The analyst can build interactive charts from event data to track suspicious activities and trends. These visualizations can be combined to form dashboards. Figure 5.4 and Figure 5.5 show visualization and dashboard respectively.

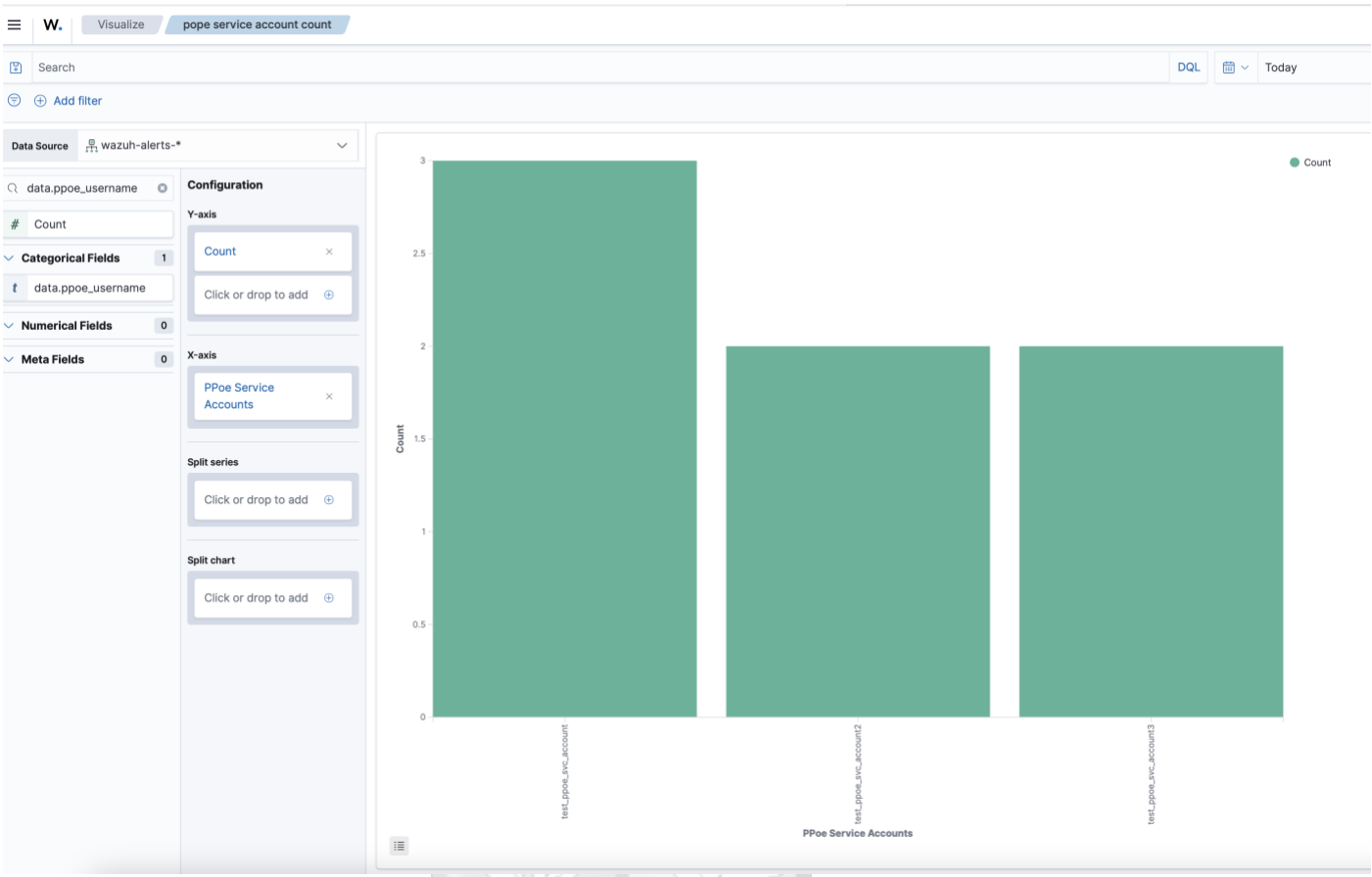


Figure 5.4: PPPoE Service Accounts by Count

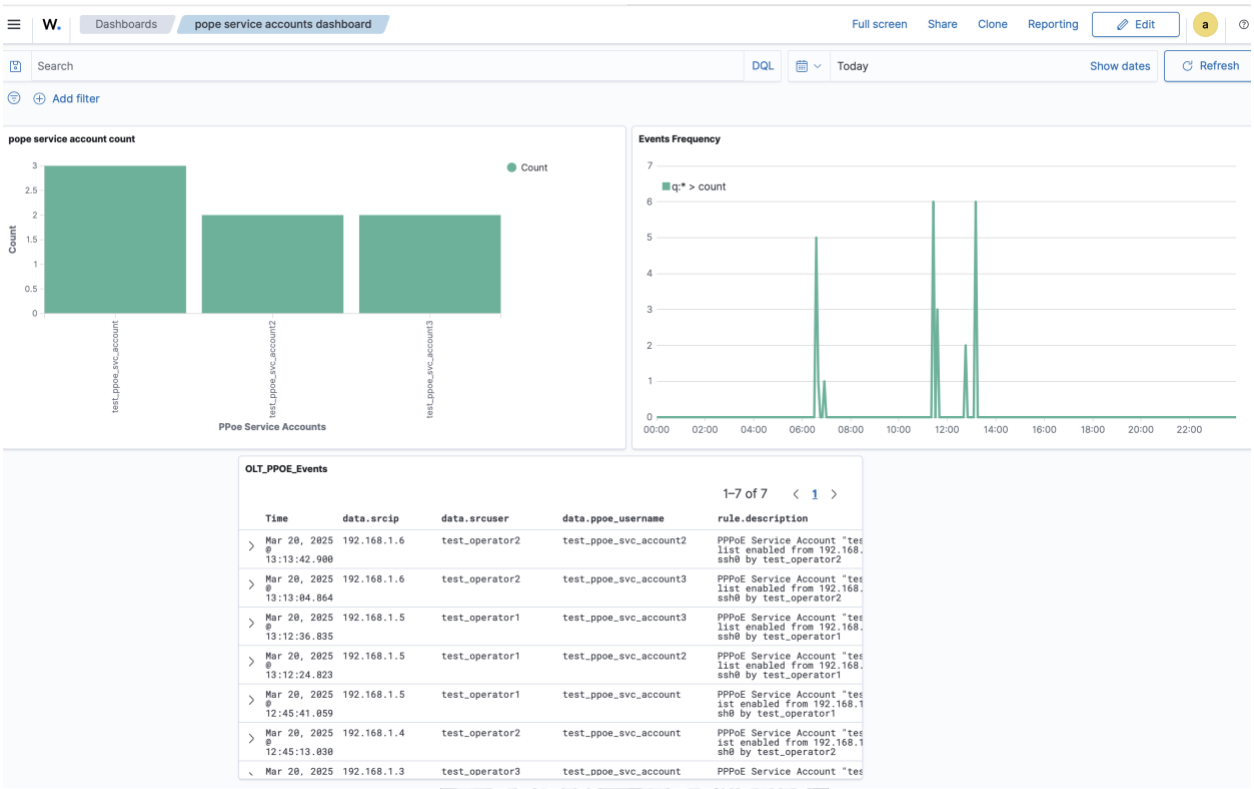


Figure 5.5: Sample PPPoE Service Accounts Dashboard

5.4 System Testing and Validation

This section describes the testing procedures for the GPON Fraud Detection system. Testing is divided into Four major areas: integration, functionality, non-functionality and compatibility testing.

5.4.1 Unit and Integration testing

In Unit Testing, individual components of the system were scrutinized to ensure that each isolated software module performs its required function. This included testing custom decoders, alert rules and integration of communication components (such as Wazuh manager/indexer and the Slack integration) in a controlled environment. Each unit was validated by confirming that it processed input logs accurately and generated the expected output.

Integration Testing was conducted after assembling the system components to verify that they functioned together seamlessly. Key aspects of this testing included:

i. Verifying that each component was operational as a unit a shown on Figure 5.6

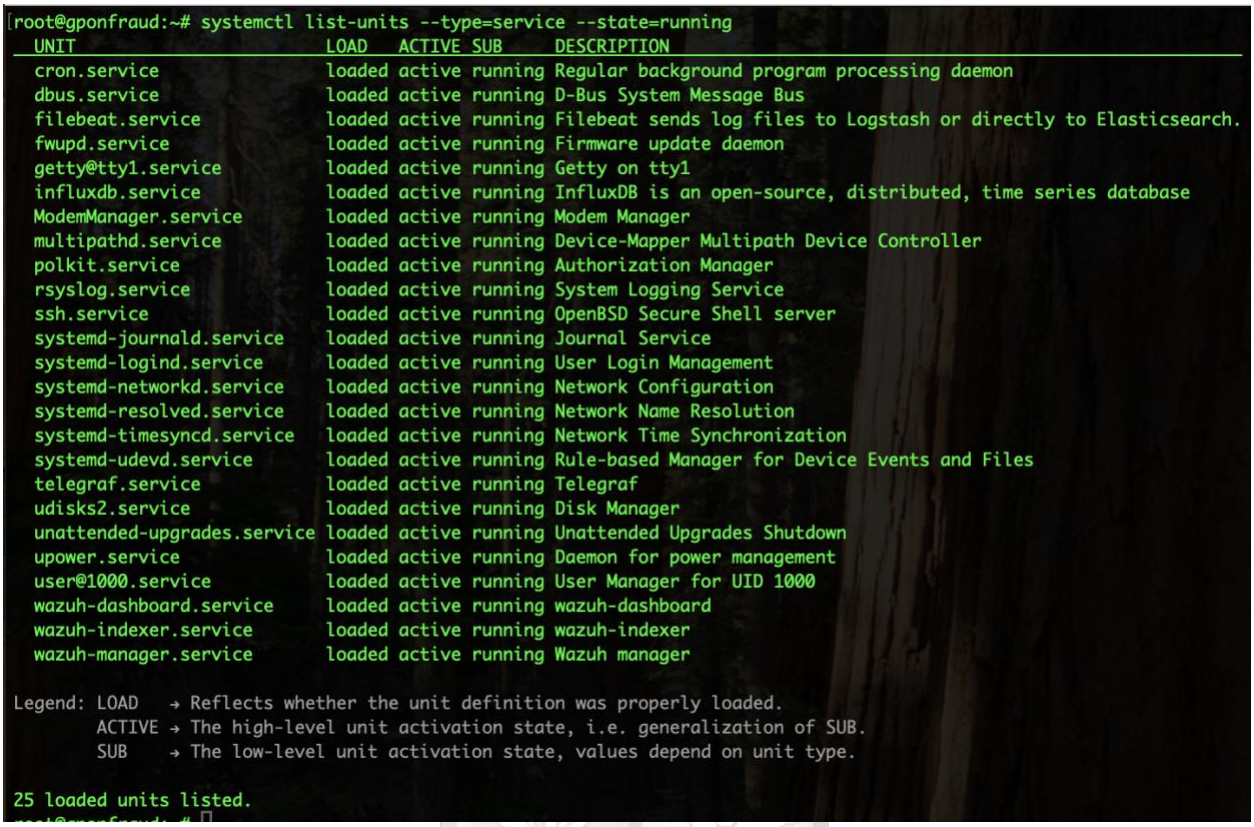


Figure 5.6: Loaded and Active Running Units

ii. Confirming if the units are integrated and corresponding service ports were open, accessible and communicating as shown in Figure 5.7.

```
root@gponfraud:~# lsof -nPi | grep -E "9200|:514|443|telegraf|influxdb"
influxd   39211        influxdb    8u  IPv6 1227566      0t0  TCP *:8086 (LISTEN)
influxd   39211        influxdb    9u  IPv6 1588982      0t0  TCP 10.15.10.5:8086->10.15.10.5:45174 (ESTABLISHED)
telegraf  46483        telegraf    6u  IPv4 1591672      0t0  TCP 10.15.10.5:45174->10.15.10.5:8086 (ESTABLISHED)
telegraf  46483        telegraf   11u  IPv4 2504503      0t0  TCP 10.15.10.5:38388->10.15.10.5:9200 (ESTABLISHED)
telegraf  46483        telegraf  262u  IPv4 1593659      0t0  TCP 10.15.10.5:52314->10.15.10.5:5066 (ESTABLISHED)
java      69811   wazuh-indexer  620u  IPv6 2503148      0t0  TCP 10.15.10.5:9200 (LISTEN)
java      69811   wazuh-indexer  639u  IPv6 3037170      0t0  TCP 10.15.10.5:9200->10.15.10.5:59338 (ESTABLISHED)
java      69811   wazuh-indexer  646u  IPv6 3037171      0t0  TCP 10.15.10.5:9200->10.15.10.5:59342 (ESTABLISHED)
java      69811   wazuh-indexer  666u  IPv6 3037172      0t0  TCP 10.15.10.5:9200->10.15.10.5:59346 (ESTABLISHED)
java      69811   wazuh-indexer  688u  IPv6 3037173      0t0  TCP 10.15.10.5:9200->10.15.10.5:59360 (ESTABLISHED)
java      69811   wazuh-indexer  954u  IPv6 2495452      0t0  TCP 10.15.10.5:9200->10.15.10.5:38388 (ESTABLISHED)
java      69811   wazuh-indexer  978u  IPv6 3040932      0t0  TCP 10.15.10.5:9200->10.15.10.5:41540 (ESTABLISHED)
java      69811   wazuh-indexer  985u  IPv6 3040933      0t0  TCP 10.15.10.5:9200->10.15.10.5:41550 (ESTABLISHED)
java      69811   wazuh-indexer  989u  IPv6 3040934      0t0  TCP 10.15.10.5:9200->10.15.10.5:41558 (ESTABLISHED)
node      82099 wazuh-dashboard   19u  IPv4 3042170      0t0  TCP *:443 (LISTEN)
node      82099 wazuh-dashboard   20u  IPv4 3047820      0t0  TCP 10.15.10.5:59338->10.15.10.5:9200 (ESTABLISHED)
node      82099 wazuh-dashboard   21u  IPv4 3042167      0t0  TCP 10.15.10.5:59342->10.15.10.5:9200 (ESTABLISHED)
node      82099 wazuh-dashboard   22u  IPv4 3042168      0t0  TCP 10.15.10.5:59346->10.15.10.5:9200 (ESTABLISHED)
node      82099 wazuh-dashboard   23u  IPv4 3042169      0t0  TCP 10.15.10.5:59360->10.15.10.5:9200 (ESTABLISHED)
node      82099 wazuh-dashboard   26u  IPv4 3049540      0t0  TCP 10.15.10.5:41540->10.15.10.5:9200 (ESTABLISHED)
node      82099 wazuh-dashboard   28u  IPv4 3049543      0t0  TCP 10.15.10.5:41550->10.15.10.5:9200 (ESTABLISHED)
node      82099 wazuh-dashboard   29u  IPv4 3049544      0t0  TCP 10.15.10.5:41558->10.15.10.5:9200 (ESTABLISHED)
wazuh-rem 82592           wazuh    4u  IPv4 3045127      0t0  UDP 10.15.10.5:514
wazuh-mod 82694            root  148u  IPv4 3052530      0t0  TCP 10.15.10.5:38080->172.67.157.37:443 (CLOSE_WAIT)
root@gponfraud:~#
```

Figure 5.7: Communicating Services

iii. Testing the end-to-end event flow from the ZTE OLT to the Wazuh platform and onward to Slack. Figure 5.8 shows OLT events being received on the Wazuh Server.

```
root@gponfraud:~# tcpdump -i any -A src net 192.168.248.12
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
15:31:06.670171 eno2  In  IP 192.168.248.12.syslog > gponfraud.syslog: SYSLOG local0.info, length: 112
E....B.....U....
.
......x..<134>2025 Apr  2 15:30:45 TEST_OLT_C300_248.12 command-log:vty0 trevor.kaon1 10.15.10.15 /*** user log in ***/

15:31:19.369435 eno2  In  IP 192.168.248.12.syslog > gponfraud.syslog: SYSLOG local0.info, length: 93
E..y.G.....c....
.
......e..<134>2025 Apr  2 15:30:57 TEST_OLT_C300_248.12 command-log:vty0 trevor.kaon1 10.15.10.15 en
```

Figure 5.8: Syslog Events from OLT to Wazuh Server

iv. Confirming that data normalization, event parsing and alert generation occurred correctly. Figure 5.9 shows sample rogue ONU registration event being normalized, parsed and firing alert rule.

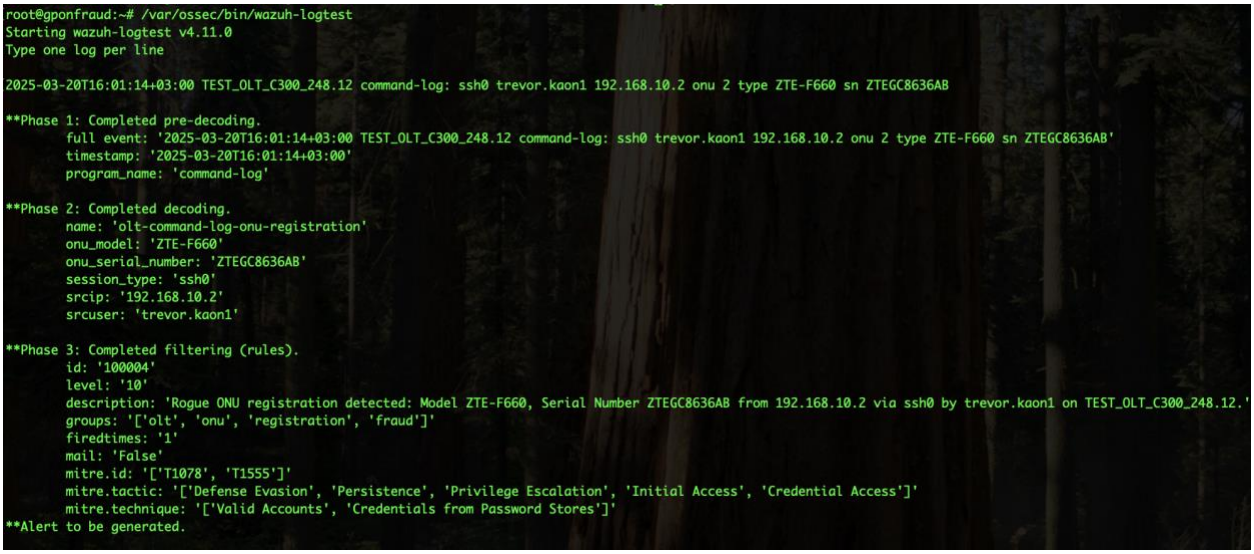


Figure 5.9: Sample Event Normalization, Parsing and Alerting

This phase was critical to ensure that all system modules work harmoniously, allowing for accurate near real-time detection of GPON fraudulent activities.

5.4.2 Functionality Testing

Testing was done by simulating fraudulent activities on the test ZTE OLT using the Netmiko Python library. The goal is to ensure that the GPON fraud detection system reliably collects, parses and alerts on these events in near real time via Slack channel.

The tests were designed to simulate realistic fraud scenarios by emulating the following events on the test ZTE OLT:

i. Simulation of rogue ONU registration.

Rogue ONU registration was simulated on the test OLT using the Appendix C (h) register_onus.py Netmiko Python script. The script registers 10 ONUs with serials starting from ZTEG12345670 to ZTEG12345679.

Serial ZTEG12345675 is added to the list of known ONUs on Wazuh server to test for false positive match in case it triggers an alert. All other serials are expected to trigger alerts. Upon simulation, the events were successfully parsed, and alerts were triggered on the Slack channel with exception of event with serial ZTEG12345675 as expected. Figure 5.10 shows a sample slack alert. The events were also visible on the Wazuh Dashboard as shown on Figure 5.11.

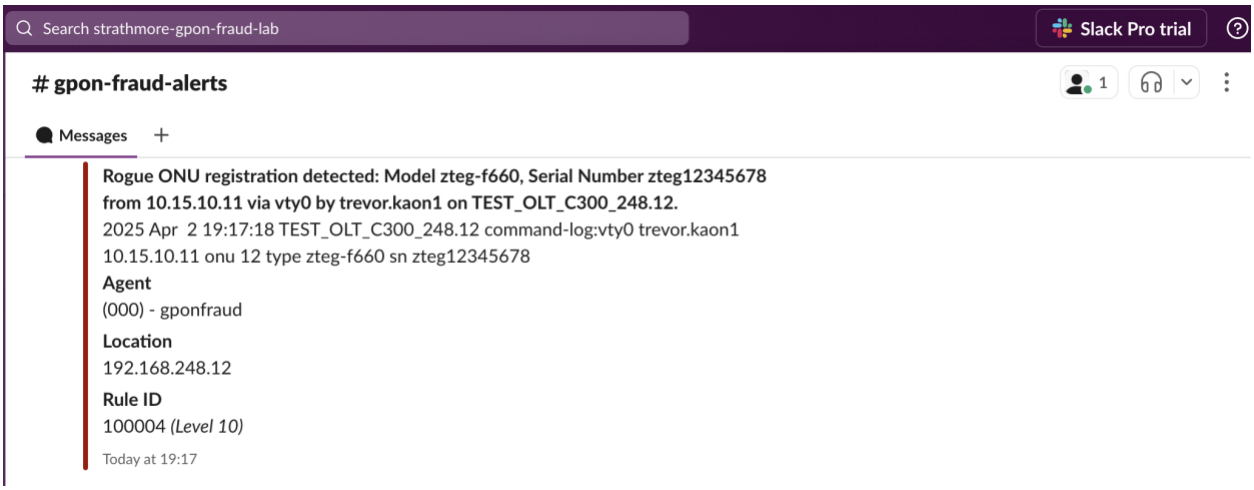


Figure 5.10: Sample Slack Rogue ONU Registration Alert

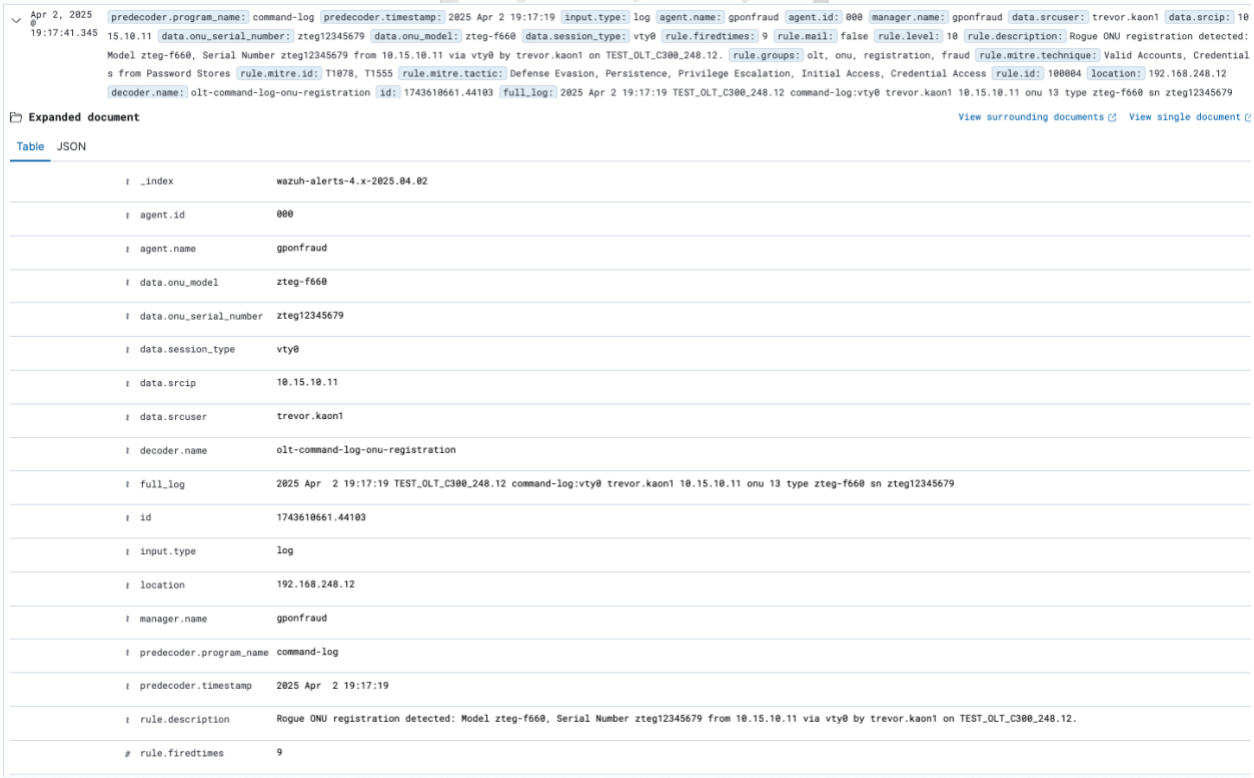


Figure 5.11: Wazuh Dashboard Rogue ONU Alert Event

ii. Simulated misuse of a zero rated PPPoE service account activity.

Registration of zero rated PPPoE service accounts was simulated using the Appendix C (i) configure_pppoe_accounts.py Netmiko Python script. The script registers 10 service accounts on an ONU interface with usernames ranging from svc_account1 to svc_account10. All the usernames are added to the watchlist with exception of svc_account5 which is expected not to trigger an alert to ensure the systems accuracy.

The events were successfully parsed triggering an alert on the Slack channel as shown by the sample alert on Figure 5.12, the events were also visible on the Wazuh Dashboard as shown on and Figure 5.13.

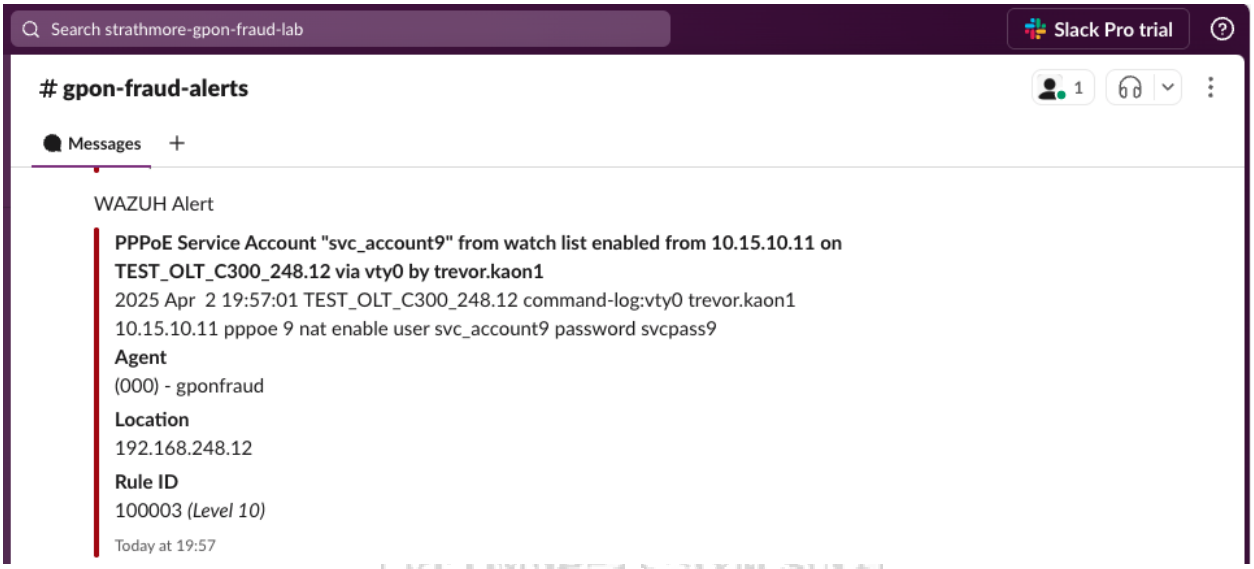


Figure 5.12: Sample PPPoE Service Account Misuse Slack Alert

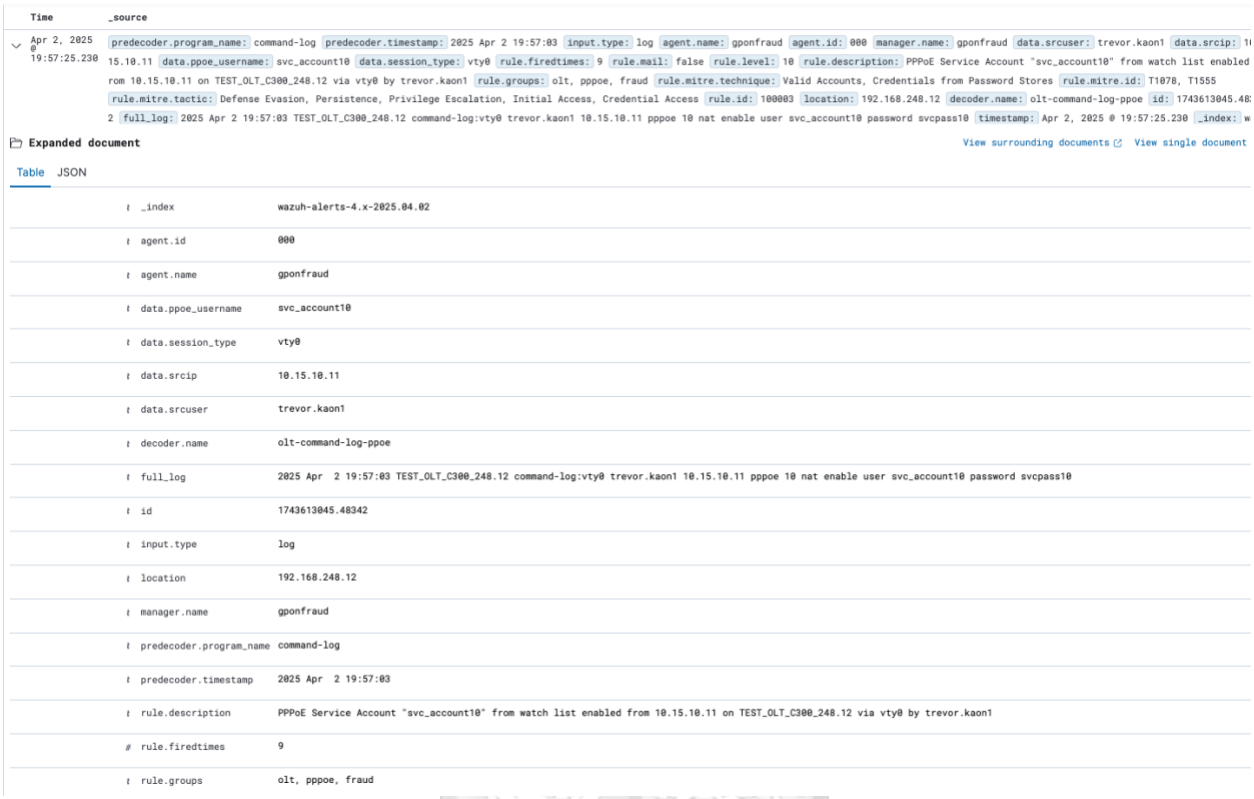


Figure 5.13: Sample Wazuh dashboard PPPoE Service Account Misuse Event

iii. Simulated unauthorized configuration of a Bandwidth profile policy.

Unauthorized configuration of a bandwidth profile was simulated using the Appendix C (j) add_bandwidth_profiles.py Netmiko Python script. The script adds 10 bandwidth profiles with names starting from test1M to test10M on the test OLT. Bandwidth profile with test5M is added to the Wazuh known bandwidths list and is expected not to trigger an alert in order to ensure system accuracy.

The events were successfully parsed, and alerts were triggered for the expected events on the Slack channel as shown by the sample alert on Figure 5.14, the associated events were also available on the Wazuh Dashboard as shown by sample event on Figure 5.15.

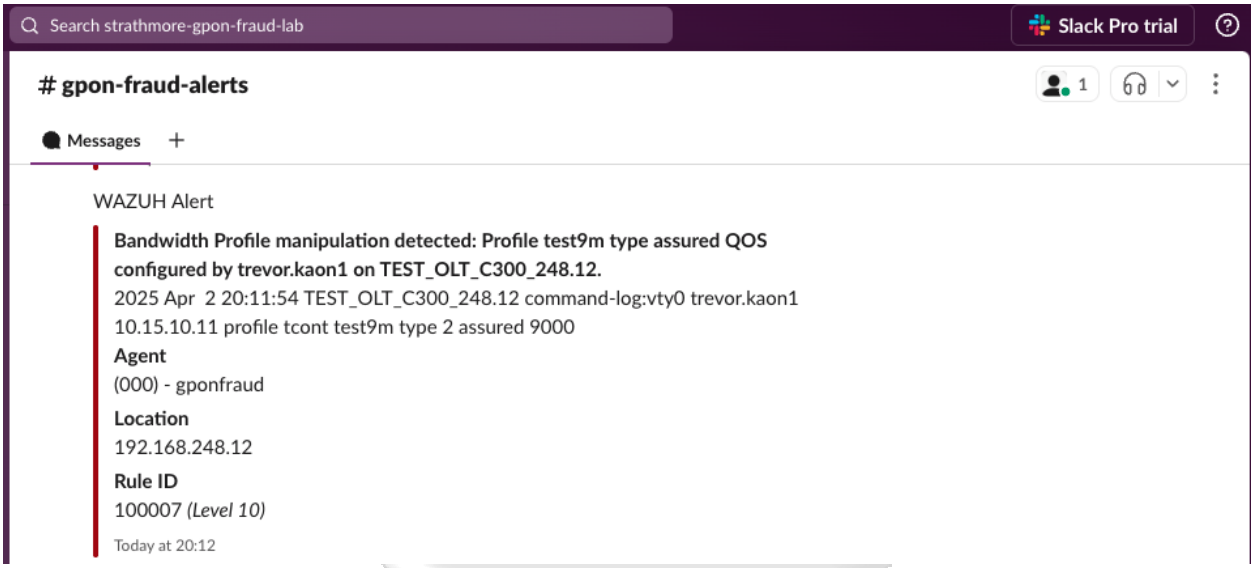


Figure 5.14: Sample Unauthorized Bandwidth Configuration Slack Alert

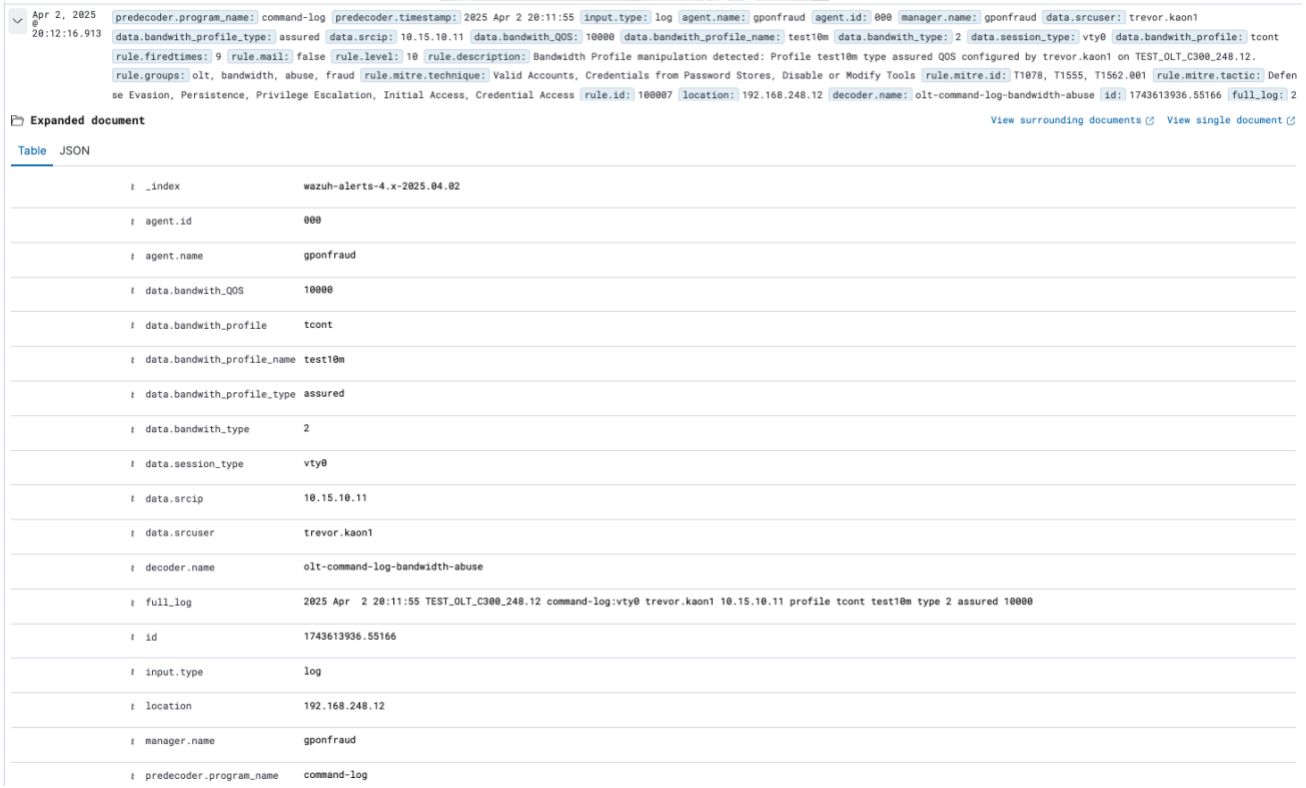


Figure 5.15: Sample Unauthorized Bandwidth Configuration Event

Each of the above activity was verified and validated by checking that:

a. The event logs were captured and indexed correctly.

b. Custom Wazuh decoders extracted the relevant fields and normalized the event data accurately.

c. Alerts were generated with the appropriate severity level and forwarded to the Slack channel with no false positives.

Table 5.1 summarizes the test results including detection accuracy and detection latency:

Table 5.1: Evaluation Summary

Test Scenario	Mean Detection Latency (s)	Detection Accuracy	Observations
Rogue ONU Registration	22.74777778	100%	Event successfully parsed, alert triggered on Slack, visible on Wazuh dashboard. No false positives
Zero-rated PPPoE Service Account Misuse	22.28344444	100%	Event successfully parsed, alert triggered on Slack, visible on Wazuh dashboard. No false positives
Unauthorized Bandwidth Configuration	22.64255556	100%	Event successfully parsed, alert triggered on Slack, visible on Wazuh dashboard. No false Positives
Alert Latency Mean of Means	22.55792593		

a. Detection Accuracy

All tests successfully identified fraudulent activities with 100% accuracy. No false positives detected.

b. Detection Latency

Alerts were triggered in near real-time within seconds. Mean alert latency for all the case scenarios was 22.55792593 seconds.

Table 5.2, Table 5.3 and Table 5.4 highlight the summaries for Rogue ONU registrations, Zero-rated PPPoE Service account misuse and Unauthorized Bandwidth configurations respectively.

Table 5.2: Rogue ONU Registrations Summary Events

Time	predecoder.timestamp	Latency (seconds)	data.onu_serial_number	Detection Accuracy
Apr 2, 2025 @ 19:17:41.345	2025 Apr 2 19:17:19	22.345	zteg12345679	100%
Apr 2, 2025 @ 19:17:40.796	2025 Apr 2 19:17:18	22.796	zteg12345678	100%
Apr 2, 2025 @ 19:17:40.266	2025 Apr 2 19:17:17	23.266	zteg12345677	100%
Apr 2, 2025 @ 19:17:39.726	2025 Apr 2 19:17:17	22.726	zteg12345676	100%
Apr 2, 2025 @ 19:17:38.590	2025 Apr 2 19:17:16	22.59	zteg12345674	100%
Apr 2, 2025 @ 19:17:38.059	2025 Apr 2 19:17:15	23.059	zteg12345673	100%
Apr 2, 2025 @ 19:17:37.522	2025 Apr 2 19:17:15	22.522	zteg12345672	100%
Apr 2, 2025 @ 19:17:36.986	2025 Apr 2 19:17:14	22.986	zteg12345671	100%
Apr 2, 2025 @ 19:17:36.440	2025 Apr 2 19:17:14	22.44	zteg12345670	100%
Mean Alert Latency		22.7477778		

Table 5.3: PPoE Service Accounts Misuse Summary Events

Time	predecoder.timestamp	Latency (s)	data.ppoe_username	Detection Accuracy
Apr 2, 2025 @ 19:57:25.230	2025 Apr 2 19:57:03	22.23	svc_account10	100%
Apr 2, 2025 @ 19:57:23.019	2025 Apr 2 19:57:01	22.019	svc_account9	100%
Apr 2, 2025 @ 19:57:20.806	2025 Apr 2 19:56:58	22.806	svc_account8	100%
Apr 2, 2025 @ 19:57:18.585	2025 Apr 2 19:56:56	22.585	svc_account7	100%
Apr 2, 2025 @ 19:57:16.376	2025 Apr 2 19:56:54	22.376	svc_account6	100%
Apr 2, 2025 @ 19:57:11.956	2025 Apr 2 19:56:50	21.956	svc_account4	100%
Apr 2, 2025 @ 19:57:09.739	2025 Apr 2 19:56:48	21.739	svc_account3	100%
Apr 2, 2025 @ 19:57:07.526	2025 Apr 2 19:56:45	22.526	svc_account2	100%
Apr 2, 2025 @ 19:57:05.314	2025 Apr 2 19:56:43	22.314	svc_account1	100%
Mean Alert Latency		22.28344444		

Table 5.4: Unauthorized Bandwidth Configuration Summary Events

Time	predecoder.timestamp	Latency (s)	data.bandwith_profile_name	data.bandwith_QOS(kbps)	Detection Accuracy
Apr 2, 2025 @ 20:41:19.753	2025 Apr 2 20:40:57	22.753	test10m	10000	100%
Apr 2, 2025 @ 20:41:19.730	2025 Apr 2 20:40:57	22.73	test9m	9000	100%
Apr 2, 2025 @ 20:41:19.706	2025 Apr 2 20:40:57	22.706	test8m	8000	100%
Apr 2, 2025 @ 20:41:19.683	2025 Apr 2 20:40:57	22.683	test7m	7000	100%
Apr 2, 2025 @ 20:41:19.655	2025 Apr 2 20:40:57	22.655	test6m	6000	100%
Apr 2, 2025 @ 20:41:19.603	2025 Apr 2 20:40:57	22.603	test4m	4000	100%
Apr 2, 2025 @ 20:41:19.579	2025 Apr 2 20:40:57	22.579	test3m	3000	100%
Apr 2, 2025 @ 20:41:19.554	2025 Apr 2 20:40:57	22.554	test2m	2000	100%
Apr 2, 2025 @ 20:41:19.520	2025 Apr 2 20:40:57	22.52	test1m	1000	100%
Mean Alert Latency		22.642556			

5.4.3 Performance Testing

Performance data collected by Telegraf from the Wazuh server such as CPU usage, memory utilization, disk I/O over the simulation period showed no notable abnormal activity. The resource utilization was efficient and optimum. Figure 5.16 shows a summary dashboard for the GPON Fraud Detection System performance.

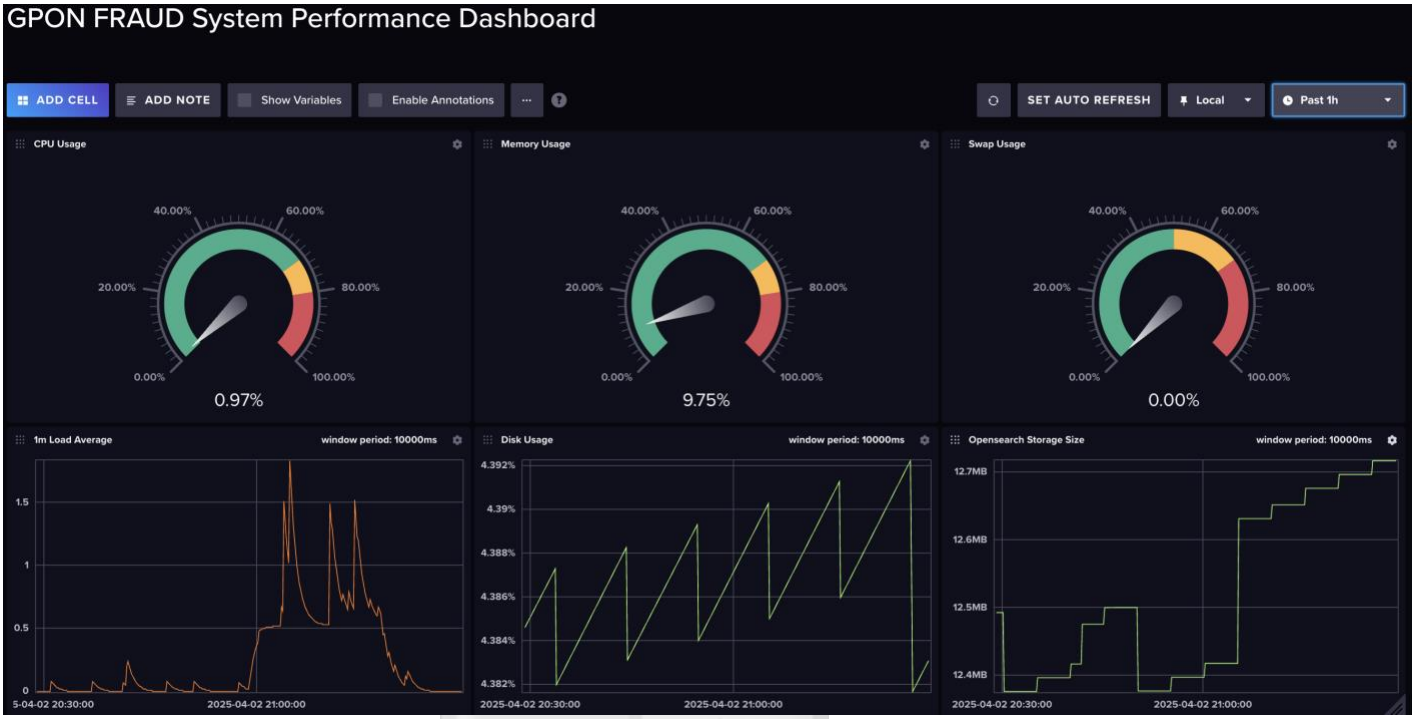


Figure 5.16: GPON FRAUD System Performance Dashboard

5.4.4 Compatibility Testing

Compatibility testing was conducted to ensure that the Wazuh Dashboard and Slack are fully compatible with the available platforms. This testing verified that the system operates seamlessly across different operating systems and web browsers configurations as shown on Table 5.5.

Table 5.5: Compatibity Tests

Browser/App	Wazuh Dashboard Compatibility	Slack Compatibility
Firefox (version 93 and above)	Yes	Yes
Chrome (version 95 and above)	Yes	Yes
Safari (version 13.7 and above)	Yes	Yes
Edge (version 95 and above)	Yes	Yes
Mobile Browsers (latest versions)	Yes	Yes
Slack App (iOS and Android)	N/A	Yes

Chapter 6: Discussions

6.1 Introduction

This chapter presents a comprehensive discussion of the findings obtained from the system development, implementation and testing and validation phases. The primary objective is to evaluate the effectiveness of the GPON fraud detection system in real-time monitoring of OLT events and ensuring quick response security against insider threats. This chapter compares the achieved results with the initial research objectives and highlights key discoveries, achievements and potential areas for improvement.

6.2 Findings and Achievements

The implemented system successfully analyzed real-time OLT logs and identified anomalies indicative of fraudulent activities. The key findings include the system's ability to process live OLT events effectively and detecting suspicious activities such as unauthorized ONT registrations, policy manipulations and unauthorized use of pppoe service accounts. The correlation engine within the system distinguished between legitimate and anomalous activities thereby minimizing false positives and improving detection accuracy. Unlike traditional GPON security solutions and mechanisms such as NMS, the developed system significantly reduced the time required to identify and flag fraudulent activities hence improving response time for mitigation.

The system demonstrated strong alerting and visualization capabilities by integrating Wazuh manager and Slack. This provided security and fraud analysts with a clear representation of security events and enabling efficient interpretation and rapid response to threats. The real-time alerting mechanism ensured immediate notifications upon the detection of anomalous activities hence facilitating prompt mitigation. Alerts were categorized based on severity levels thereby ensuring that high-risk events were prioritized for swift resolution.

Another significant aspect of the findings was the role of Slack in network monitoring. The system revealed earlier gaps in real-time event analysis where some fraudulent activities could remain undetected due to delays in alerting mechanisms. By implementing enhanced correlation logic and optimizing alerting structures, the system effectively mitigated these lapses thus ensuring that fraud detection was both timely and comprehensive. The accuracy of fraudulent activity detection was also validated with high detection rates for unauthorized activity hence ensuring integrity and preventing resource abuse.

In terms of system performance and scalability, the event processing mechanism efficiently handled the log entries without degradation. Performance tests indicated minimal latency in event correlation and alert generation thus making the system viable for large-scale deployments across multiple OLTs and ONUs. Additionally, the system demonstrated its possibility to scale within dynamic ISP environments with multiple network components. This ensures that fraudulent activities could be detected across various operational scenarios.

6.3 Evaluation of Objectives

The study's results were assessed against the initial research objectives. In understanding the characteristics of fraudulent activities, the study successfully identified key fraud patterns such as rogue ONU registrations, unauthorized access account provisioning and policy manipulation. Detailed analysis of fraud characteristics provided insights into behavioral patterns and assisted in refining detection rules.

The evaluation of existing GPON security solutions revealed that conventional methods lacked real-time correlation capabilities hence underscoring the necessity of the developed system. Significant gaps were identified in traditional mechanisms particularly in addressing insider threats within GPON environments. The system incorporated correlation rules tailored to detect GPON specific fraud patterns, ensuring high detection accuracy. Simulated attack scenarios validated the robustness of the system in real world applications.

System testing and validation confirmed that the developed solution performed as expected in effectively identifying and mitigating fraudulent activities. The Fraud detection systems showcased superior accuracy and response time.

6.4 Challenges and Limitations

Vendor specific limitations arose since the system was tested exclusively on ZTE based OLTs which initially limited its generalizability to other vendors. However, scalability is achievable due to the system's flexibility in developing custom decoders that can capture diverse fraud activities or specific use cases across different GPON infrastructures. By implementing tailored decoders, the system can dynamically adapt to varying vendor specific log formats thereby enhancing its compatibility and making it a viable solution for broader adoption in diverse operational environments. Future enhancements should incorporate multi-vendor support to improve

applicability across different GPON infrastructures. Expanding compatibility would enable wider adoption of the system and enhance its effectiveness in diverse operational environments.

While the system demonstrated scalability in a controlled test environment, the real-world deployment across a distributed ISP infrastructure may introduce additional complexities that require further evaluation. Large scale deployments might necessitate additional refinements in data storage, retrieval efficiency and real-time analytics performance.

6.5 Implications of findings

The findings of this study demonstrate the feasibility of leveraging real-time log analysis for fraud detection in GPON networks. The system provides a proactive security layer that can be integrated into ISP operations to enhance network integrity and protect against insider threats. The ability to detect fraudulent activities in real time enables service providers to take immediate remedial actions hence reducing financial losses and ensuring service continuity.

The adoption of the developed fraud detection system can help ISPs minimize financial losses due to fraud, improve regulatory compliance and enhance customer trust. The study confirms that real-time fraud detection significantly strengthens the security posture of GPON networks by identifying suspicious activities before they escalate into major security breaches.

Chapter 7: Conclusions, Recommendations and Future Work

7.1 Conclusions

This dissertation has examined the issue of GPON fraud and developed a real-time fraud detection system based on OLT event processing. The research successfully identified key fraud patterns, evaluated existing security solutions and designed a system that enhances real-time fraud detection capabilities. The results demonstrated that real-time log analysis and correlation significantly improve the ability to detect and mitigate fraudulent activities within GPON networks.

The study found that insider threats remain a significant challenge in GPON environments, where authorized network operators can manipulate configurations to bypass security measures. The developed system effectively mitigated this risk by analyzing operator activities, detecting anomalies and providing real-time alerts. The research also revealed that traditional solution such as NMSs lack comprehensive event correlation, making them ineffective against sophisticated fraud schemes. The developed system addressed this gap by leveraging real-time log processing, visual analytics and automated alerting mechanisms.

Despite the system's success, vendor-specific constraints exists due to usage of only ZTE OLT. However, the system's adaptability and ability to integrate custom decoders suggest strong potential for scalability across different GPON OLTs and infrastructures. The findings confirm that proactive fraud detection mechanisms are essential for protecting GPON networks and ensuring service integrity for Internet Service Providers.

7.2 Recommendations

Based on the findings of this research, the following recommendations are proposed:

i. Enhanced Machine Learning Integration

Future versions of the fraud detection system should incorporate machine learning models to improve anomaly detection accuracy and adapt to evolving fraud patterns.

ii. Multi-Vendor Compatibility

The system should be extended to support OLTs from multiple vendors, ensuring broader applicability and increased adoption across different network infrastructures.

iii. Improved Resource Optimization

Given the high volume of log events processed, efforts should be made to optimize system performance through distributed processing and efficient log storage mechanisms.

iv. Automation of Fraud Response

To further strengthen fraud mitigation, automated response mechanisms should be integrated, allowing the system to take predefined actions when suspicious activities are detected.

v. Regulatory Compliance and Standardization

ISPs should align fraud detection mechanisms with regulatory frameworks and industry best practices to enhance network security and compliance.

vi. User Awareness and Training

Since insider threats play a significant role in GPON fraud, ISPs should invest in training programs for network administrators and operators to promote ethical practices and awareness of fraud detection mechanisms.

7.3 Future Work

While this research has made significant contributions to GPON fraud detection, there are several areas for future improvement:

i. Cloud-Based Fraud Detection Solutions

Deploying fraud detection as a cloud-based service could improve scalability, accessibility, and flexibility, enabling ISPs to monitor fraud activity across multiple geographic locations.

ii. Expansion to Other Network Technologies

The current system is designed for GPON networks, however, similar real-time fraud detection mechanisms could be developed for other fiber-optic and broadband technologies, such as EPON and XG-PON.

iii. Real-World Implementation and Testing

Further testing in live ISP environments is necessary to validate system performance and assess the overall impact on fraud mitigation.

7.4 Final Remarks

This dissertation contributes to the advancement of fraud detection in GPON networks by presenting a robust, real-time detection mechanism. The developed system has demonstrated effectiveness in detecting fraudulent activities and addressed existing gaps in GPON fraud detection thus providing ISPs with a proactive approach to network security. While challenges remain, continuous improvements and future research will further enhance the system's capabilities in ensuring a more secure and resilient GPON infrastructure.

References

Ajmal, T., Hugues-Salas, E., Razavi, R., Quinlan, T., Zervas, G., Simeonidou, D., & Walker, S. D. (2007). Phase-Encrypted Secure Communication technique for GPONs. *2007 Photonics in Switching*, 103–104. https://doi.org/10.1109/PS.2007.4300765

Cisco Systems. (2020). *Getting Started With OLT Network Configuration, Cisco Catalyst PON Series Switches*. Cisco Systems.

Cisco Systems. (2024, May 8). *Compare TACACS + and RADIUS*. Cisco Systems.

FTTH Council Europe. (2024). *Everything you need to know about FTTH*.

Gal Zror. (2022). Hacking ISPs with Point-to-Pwn Protocol over Ethernet (PPPoE). *DEF CON 30*.

Gutierrez, D., Cho, J., & Kazovsky, L. G. (2007). TDM-PON Security Issues: Upstream Encryption is Needed. *OFC/NFOEC 2007 - 2007 Conference on Optical Fiber Communication and the National Fiber Optic Engineers Conference*, 1–3. https://doi.org/10.1109/OFC.2007.4348474

Hongjian Guo. (2015). *Gigabit-capable passive optical network (GPON) system and point-to-point protocol over Ethernet (PPPOE) configuration method implemented thereby*. Google Patents.

Horvath, T., Malina, L., & Munster, P. (2015). On security in gigabit passive optical networks. *2015 International Workshop on Fiber Optics in Access Network (FOAN)*, 51–55. https://doi.org/10.1109/FOAN.2015.7320479

Horvath, T., Munster, P., Oujezsky, V., Vojtech, J., Holik, M., Dejdar, P., & Latal, M. (2019). GPON Network with Simulated Rogue ONU. *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 1–5. https://doi.org/10.23919/SOFTCOM.2019.8903811

Huawei. (2013). *iManager U2000 Unified Network Management System V100R009C00*. http://www.huawei.com

Huawei. (2023). Broadband Remote Access Server (BRAS). In Guo Yuhan (Ed.), *IP Encyclopedia*. Huawei.

iMaster NCE V100R019C00 Product Description (Access Domain, ARM). (2021). https://www.huawei.com

International Telecommunication Union. (n.d.). *ONU management and control interface (OMCI) specification ITUPublications International Telecommunication Union*. http://handle.itu.int/11.1002/1000/11830-en.

International Telecommunication Union. (2008). *ITU-T Rec. G.984.1 (03/2008) Gigabit-capable passive optical networks (GPON): General characteristics*.

Liu, Y., Zhang, G., & Li, Q. (2011). WDM/TDM Hybrid GPON Technology. *2011 Symposium on Photonics and Optoelectronics (SOPO)*, 1–3. https://doi.org/10.1109/SOPO.2011.5780515

Malina, L., Munster, P., Hajny, J., & Horvath, T. (2015). Towards secure Gigabit Passive Optical Networks: Signal propagation based key establishment. *2015 12th International Joint Conference on E-Business and Telecommunications (ICETE)*, *04*, 349–354.

Nathan Pan, A. T. (2023, December 6). *Understand GPON Technology*. Cisco Systems.

Resecurity. (2024). *Hundreds of network operators' credentials found circulating in the Dark Web*.

Selmanovic, F., & Skaljo, E. (2010). GPON in Telecommunication Network. *International Congress on Ultra Modern Telecommunications and Control Systems*, 1012–1016. https://doi.org/10.1109/ICUMT.2010.5676500

Vinh, T. Q., Park, J.-H., Kim, Y.-C., & Kim, K.-O. (2008). An FPGA implementation of 30Gbps security module for GPON systems. *2008 8th IEEE International Conference on Computer and Information Technology*, 868–872. https://doi.org/10.1109/CIT.2008.4594788

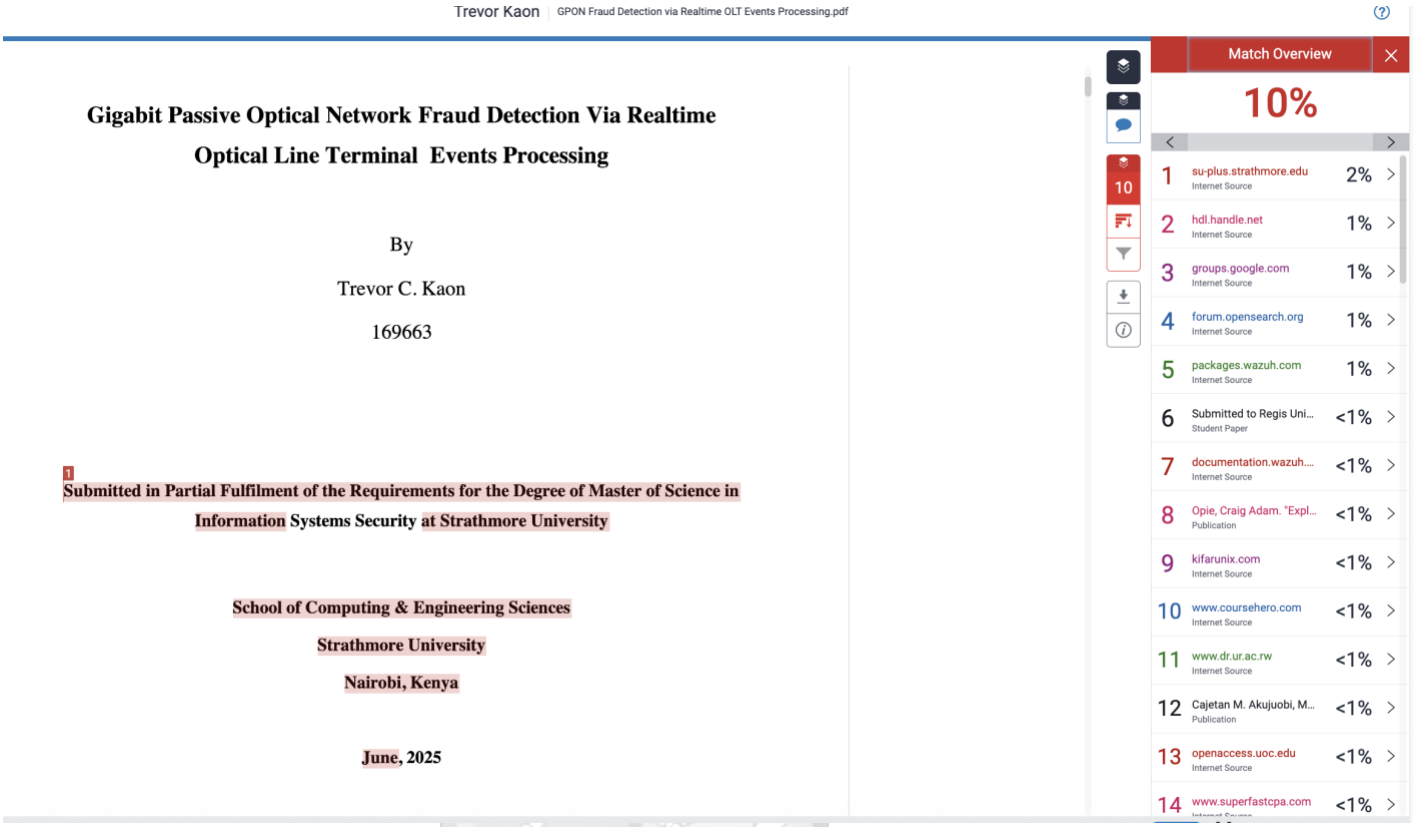
Yang, L., Zhang, Q., Huang, Z., & Zhang, W. (2020). Dynamic Bandwidth Allocation (DBA) Algorithm for Passive Optical Networks. *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, 1–6. https://doi.org/10.1109/ITNAC50341.2020.9315119

ZTE. (2021). *NetNumen™ U31 R18 Unified Element Management System Security Management Operation Guide LEGAL INFORMATION*.

ZTE. (2024). *ZXA10 C600/C650/C620 Optical Access Convergence Equipment Security Description*.

Appendices

Appendix A: Similarity Report



Appendix B: Ethical Clearance Confirmation

Strathmore UNIVERSITY

2nd April 2025

Mr Kaon Trevor,
trevor.kaon@strathmore.edu

Dear Mr Kaon,

RE: GPON Fraud Detection via Real-Time OLT Events Processing

This is to inform you that SU-ISERC has reviewed and **approved** your above **SU-masters** proposal. Your application reference number is **SU-ISERC2762/25.** The approval period is from **2nd April 2025 to 1st April 2026.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
iv. Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 72 hours.
v. Clearance for the export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days of completion of the study to SU-ISERC.

Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

Mr Ambrose Rachier,
Chairperson; SU-ISERC

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email admissions@strathmore.edu www.strathmore.edu

Appendix C: Configuration files and Scripts

a. Wazuh Indexer configuration file (opensearch.yml)

```
network.host: "10.15.10.5"
node.name: "node-1"
cluster.initial_master_nodes:
- "node-1"
#- "node-2"
#- "node-3"
cluster.name: "wazuh-cluster"
#discovery.seed_hosts:
#  - "node-1-ip"
#  - "node-2-ip"
#  - "node-3-ip"
node.max_local_storage_nodes: "3"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-
ca.pem
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false

plugins.security.authcz.admin_dn:
- "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.nodes_dn:
- "CN=node-1,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-2,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-3,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.restapi.roles_enabled:
- "all_access"
- "security_rest_api_access"

plugins.security.system_indices.enabled: true
plugins.security.system_indices.indices: [".plugins-ml-model", ".plugins-ml-task",
".opendistro-alerting-config", ".opendistro-alerting-alert*", ".opendistro-anomaly-
```

```
results*", ".opendistro-anomaly-detector*", ".opendistro-anomaly-checkpoints",
".opendistro-anomaly-detection-state", ".opendistro-reports-*", ".opensearch-
notifications-*", ".opensearch-notebooks", ".opensearch-observability", ".opendistro-
asynchronous-search-response*", ".replication-metadata-store"]

### Option to allow Filebeat-oss 7.10.2 to work ###
compatibility.override_main_response_version: true
```

b. Filebeat Configuration file (filebeat.yml)

```
# Wazuh - Filebeat configuration file
output.elasticsearch:
  hosts: ["10.15.10.5:9200"]
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/filebeat.pem"
  ssl.key: "/etc/filebeat/certs/filebeat-key.pem"
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false

#Filebeat HTTP Endpoint for Metrics
http.enabled: true
http.host: 10.15.10.5
http.port: 5066

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: false

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
```

```
  keepfiles: 7
  permissions: 0644

logging.metrics.enabled: false

seccomp:
  default_action: allow
  syscalls:
  - action: allow
    names:
    - rseq
```

c. Wazuh Dashboard configuration file (opensearch_dashboards.yml)

```
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://10.15.10.5:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersAllowlist: ["securitytenant","Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wz-home
```

d. Custom decorders configuration file (local_decorder.xml)

```
 <!-- Local Decoders -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!--
  - Allowed static fields:
  - location   - where the log came from (only on FTS)
  - srcuser    - extracts the source username
  - dstuser    - extracts the destination (target) username
  - user       - an alias to dstuser (only one of the two can be used)
  - srcip      - source ip
```

```
 - dstip      - dst ip
 - srcport    - source port
 - dstport    - destination port
 - protocol   - protocol
 - id         - event id
 - url        - url of the event
 - action     - event action (deny, drop, accept, etc)
 - status     - event status (success, failure, etc)
 - extra_data - Any extra data
-->

<decoder name="local_decoder_example">
   <program_name>local_decoder_example</program_name>
   </decoder>

<decoder name="olt-command-log-pppoe">
          <program_name>command-log</program_name>
          <prematch
type="pcre2">^.*?\d*\s+\S+\s+\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s+pppoe\s+\d+\s+nat
enable user \S+\s+password\s+.*</prematch>
   <regex
type="pcre2">.*?(ssh\d*|vty\d*)\s+(\S+)\s+(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s+pppoe\
s+\d+\s+nat enable user (\S+)\s+password\s+.*</regex>
   <order>session_type, srcuser, srcip, pppoe_username</order>
</decoder>


<decoder name="olt-command-log-onu-registration">
       <program_name>command-log</program_name>
       <prematch
type="pcre2">^.*?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s+onu\s+\d+\stype\s\S+\s+sn\s+\S+
</prematch>
   <regex
type="pcre2">^.*?(ssh\d*|vty\d*)\s+(\S+)\s+(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s+onu\s
+\d+\stype\s(\S+)\s+sn\s+(\S+)</regex>
   <order>session_type, srcuser, srcip, onu_model, onu_serial_number</order>
</decoder>


<decoder name="olt-command-log-uservlan-abuse">
       <program_name>command-log</program_name>
       <prematch
type="pcre2">.*?\d*\s+\S+\s+\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s+service-
port\s\d+\s+vport\s\d+\s+user\-vlan\s+\S+.*</prematch>
```

```
      <regex
type="pcre2">.*?(ssh\d*|vty\d*)\s+(\S+)\s+(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s+service
-port\s\d+\s+vport\s\d+\s+user\-vlan\s+(\S+).*</regex>
   <order>session_type, srcuser, srcip, user_vlan_id</order>
</decoder>
```

e. Custom rules configuration file (local_rules.xml)

```
 <!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

 <!--
 Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
 -->
 <rule id="100001" level="5">
  <if_sid>5716</if_sid>
  <srcip>1.1.1.1</srcip>
  <description>sshd: authentication failed from IP 1.1.1.1.</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
 </rule>

</group>

<group name="olt,pppoe,fraud">
 <rule id="100003" level="10">
  <decoded_as>olt-command-log-pppoe</decoded_as>
  <list field="pppoe_username"
lookup="match_key">etc/lists/pppoe_service_accounts</list>
  <description>PPPoE Service Account "$(pppoe_username)" from watch list enabled
from $(srcip) on $(hostname) via $(session_type) by $(srcuser)</description>
  <mitre>
   <id>T1078</id>
   <id>T1555</id>
  </mitre>
 </rule>
</group>

<group name="olt,onu,registration,fraud">
 <rule id="100004" level="10">
      <decoded_as>olt-command-log-onu-registration</decoded_as>
```

```
        <list field="onu_serial_number"
lookup="not_match_key">etc/lists/authorized_onus</list>
    <description>Rogue ONU registration detected: Model $(onu_model), Serial Number
$(onu_serial_number) from $(srcip) via $(session_type) by $(srcuser) on
$(hostname).</description>
    <mitre>
      <id>T1078</id>
      <id>T1555</id>
    </mitre>
  </rule>
</group>

<group name="olt,uservlan,abuse,fraud">
  <rule id="100006" level="10">
        <decoded_as>olt-command-log-uservlan-abuse</decoded_as>
    <list field="user_vlan_id" lookup="match_key">etc/lists/service_uservlans</list>
    <description>User VLAN policy manipulation detected: VLAN ID $(user_vlan_id)
from $(srcip) via $(session_type) by $(srcuser) on $(hostname).</description>
    <mitre>
      <id>T1078</id>
      <id>T1555</id>
      <id>T1562.001</id>
    </mitre>
  </rule>
</group>
```

f. InfluxDB configuration file (config.toml)

```
bolt-path = "/var/lib/influxdb/influxd.bolt"
engine-path = "/var/lib/influxdb/engine"
```

g. Telegraf configuration file (telegraf.conf)

```
 [[outputs.influxdb_v2]]
   urls = ["http://10.15.10.5:8086"]
   token =
"4uEcTB9Zickl8nuYzpADs3jJDgKiWy2lnsX8nc_V5wYJb4kyQahBWhhws3QWvQkE
CUxI7c5bo8PDrE0XbVDr8A=="
   organization = "gpon-fraud-lab"
   bucket = "gponfraud"

 [[inputs.procstat]]
  systemd_unit = "wazuh-manager.service"
```

```
 include_systemd_children = true

[[inputs.procstat]]
 systemd_unit = "filebeat.service"
 include_systemd_children = true

[[inputs.http]]
 urls = ["http://10.15.10.5:5066/stats"]
 method = "GET"
 data_format = "json_v2"

[[inputs.elasticsearch]]
 servers = ["https://10.15.10.5:9200"]
 username = "admin"
 password = "admin"
 tls_ca = "/etc/telegraf/root-ca.pem"
 insecure_skip_verify = true
 local = true
 cluster_health = false
 cluster_stats = false
 cluster_stats_only_from_master = true
 indices_include = ["_all"]
 indices_level = "shards"
```

h. register_onus.py

Custom Netmiko Python script to simulate registration of 10 ONUs on the test OLT.

```
from netmiko import ConnectHandler

# Define OLT connection details
zte_olt = {
    "device_type": "zte_zxros",
    "host": "192.168.1.12",  # Change to your OLT IP
    "username": "admin",     # Change to your OLT username
    "password": "XXXXX",  # Change to your OLT password
    "secret": "XXXX",  # Change to your enable password
}

# GPON Interface
gpon_port = "gpon-olt_1/3/1"

# ONU Serial Number Range
start_sn = 70  # Start from ZTEG12345670
end_sn = 79    # End at ZTEG12345679
```

```
onu_type = "ZTEG-F660"  # ONU Type

try:
    net_connect = ConnectHandler(**zte_olt)
    print("Connected to OLT successfully.")

    # Enter enable mode
    net_connect.enable()
    print("Entered enable mode.")

    # Enter configuration mode
    commands = ["configure terminal", f"interface {gpon_port}"]

    # Loop to add ONUs
    onu_id = 4  # Start ONU ID from 4
    for sn_suffix in range(start_sn, end_sn + 1):
        serial_number = f"ZTEG123456{sn_suffix}"  # Generate ONU serial number
        onu_command = f"onu {onu_id} type {onu_type} sn {serial_number}"
        commands.append(onu_command)
        print(f"Configuring ONU {onu_id}: Type {onu_type}, SN {serial_number}")
        onu_id += 1  # Increment ONU ID

    # Exit config mode and save changes
    commands.extend(["exit", "exit", "write"])

    # Send commands
    output = net_connect.send_config_set(commands, exit_config_mode=False)
    print(output)

    # Disconnect
    net_connect.disconnect()
    print("Configuration complete. Disconnected from OLT.")
```

i. configure_pppoe_accounts.py

Custom Netmiko Python script to simulate configuration of 10 pppoe accounts to an ONU interface on the test OLT

```
from netmiko import ConnectHandler

# Define OLT connection details
zte_olt = {
    "device_type": "zte_zxros",
    "host": "192.168.1.12",  # Change to your OLT IP
    "username": "admin",     # Change to your OLT username
    "password": "XXXXX",  # Change to your OLT password
```

```
    "secret": "XXX",  # Change to your enable password
    "global_delay_factor": 3  # Handle slow OLT response
}

# ONU Interface
onu_mng_interface = "gpon-onu_1/3/1:4"

# Connect to OLT
net_connect = ConnectHandler(**zte_olt)
print("Connected to OLT successfully.")

# Enter enable mode
net_connect.enable()
print("Entered enable mode.")

# Enter ONU management mode
net_connect.send_command_timing("configure terminal")
net_connect.send_command_timing(f"pon-onu-mng {onu_mng_interface}")

# Configure multiple PPPoE accounts (svc_account1 to svc_account10)
for i in range(1, 11):
    pppoe_user = f"svc_account{i}"
    pppoe_pass = f"svcpass{i}"
    command = f"pppoe {i} nat enable user {pppoe_user} password {pppoe_pass}"

    print(f"Configuring {pppoe_user}...")
    net_connect.send_command_timing(command)  # Send command without waiting for a response

# Exit and save configuration
net_connect.send_command_timing("exit")
net_connect.send_command_timing("exit")
net_connect.send_command_timing("write")

# Disconnect
net_connect.disconnect()
print("Configuration complete. Disconnected from OLT.")
```

j. add_bandwidth_profiles.py

Custom Netmiko Python script to simulate addition of 10 bandwidth service profiles on the test OLT

```
from netmiko import ConnectHandler

# --- OLT Connection Details (Modify as needed) ---
zte_olt = {
```

```
    "device_type": "zte_zxros",
    "host": "192.168.1.12",  # <--- CHANGE TO YOUR OLT IP
    "username": "admin",     # <--- CHANGE TO YOUR OLT USERNAME
    "password": "XXXXXXX",  # <--- CHANGE TO YOUR OLT PASSWORD
    "secret": "XXXXX",       # <--- CHANGE TO YOUR OLT ENABLE PASSWORD
}

# Connect to OLT
try:
    print(f"Connecting to OLT {zte_olt['host']}...")
    net_connect = ConnectHandler(**zte_olt)
    print("Connected successfully.")

    # Enter enable mode
    if zte_olt.get("secret"):
        net_connect.enable()
        print("Entered enable mode.")

    # --- Generate commands for multiple T-CONT profiles ---
    config_commands = [
        "configure terminal",
        "gpon",                      # Enter GPON context
    ]

    # Loop to create profiles test1M to test10M
    for i in range(1, 11): # Generates numbers 1 through 10
        profile_name = f"test{i}M"
        assured_bandwidth = i * 1000 # 1*1000=1000, 2*1000=2000, ..., 10*1000=10000
        profile_command = f"profile tcont {profile_name} type 2 assured {assured_bandwidth}"
        config_commands.append(profile_command)
        print(f"Generated command: {profile_command}") # Optional: view generated commands

    # Add commands to exit contexts and save
    config_commands.extend([
        "exit",                      # Exit GPON context
        "exit",                      # Exit configuration mode
        "write",                      # Save configuration
    ])
    # --- End command generation ---

    # Send configuration commands
    print("\nSending configuration commands...")
    # Using send_config_set as it handles multiple commands well
    output = net_connect.send_config_set(config_commands)

    print("\n--- OLT Output ---"
```

Appendix D: Installation of System Components.

This appendix provides a step-by-step installation guide for deploying Wazuh in a GPON Fraud Detection environment. The setup includes Wazuh Indexer, Wazuh Manager and Wazuh Dashboard on an Ubuntu 22.04 LTS server. Additionally, it covers configuration and integration of Slack and performance monitoring tools.

System Requirements

Before proceeding with the installation, ensure that your system meets the following minimum hardware requirements:

i. Hardware Recommendations:

Component	Minimum	Recommended
RAM (GB)	4	16
CPU (cores)	2	8

ii. Disk Space and Operating System Requirements:

The required disk space depends on the number of endpoints and the volume of alerts generated. For detailed storage calculations, refer to the [Wazuh Indexer Hardware Recommendations]

Wazuh supports the following 64-bit Linux distributions:

- Amazon Linux 2, Amazon Linux 2023
- CentOS 7, 8
- Red Hat Enterprise Linux 7, 8, 9
- Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Installation Steps

i. Update and Prepare the System

Before installing Wazuh, update the system to ensure all packages are up to date.

```
sudo apt update && sudo apt upgrade -y
sudo apt install curl apt-transport-https unzip wget -y
```

ii. Install and Configure Wazuh Indexer

The Wazuh Indexer is based on OpenSearch and is responsible for storing and indexing security events. Step by Step guide can found from the official documentation below:

https://documentation.wazuh.com/current/installation-guide/wazuh-indexer/step-by-step.html

iii. Install and Configure Wazuh Server (Filebeat and Wazuh Manager)

The Wazuh server is a central component that includes the Wazuh manager and Filebeat.

Step-by-Step guide can found from the official documentation below:

https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html

Step 3: Install and Configure Wazuh Dashboard

A Step-by-Step guide to install and configure Wazuh Dashboard can be found from the official documentation:

https://documentation.wazuh.com/current/installation-guide/wazuh-dashboard/step-by-step.html

iv. Setting Up a Slack Incoming Webhook

Before configuring Wazuh to send alerts to Slack, you must first create an Incoming Webhook in your Slack workspace:

Step 1: Create a Slack App

a. Go to Slack API: Applications and click Create New App.

b. Give your app a name (e.g., “Wazuh Alerts”) and select the workspace where you want the alerts delivered.

Step 2: Enable Incoming Webhooks

a. In your app’s settings, navigate to Incoming Webhooks.

b. Toggle the switch to Enable Incoming Webhooks.

Step 3: Create a Webhook URL

a. Click Add New Webhook to Workspace.

b. Choose the channel where you want alerts posted and authorize the integration.

c. Slack will generate a webhook URL that looks similar to: https://hooks.Slack.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX

d. Save this URL—it will be used in your Wazuh configuration.

The following XML snippet defines the Slack integration for Wazuh. It specifies the webhook URL, the JSON alert format, and filters to forward only the high-severity alerts from specific groups and rule IDs. Modify the intergration section of the Wazuh config and use the Slack webhook URL generated in step 3 above.

```
<!-- Sample Slack Integration Template for Wazuh Alerts -->
<integration>
  <name>Slack</name>
  <hook_url>https://hooks.Slack.com/services/XXX/YYY/ZZZZ</hook_url>
  <alert_format>json</alert_format>
  <!-- Optional Filters -->
  <rule_id>10000</rule_id>
  <level>10</level>
  <group> </group>
</integration>
```

iv. Installation and configuring of performance monitoring tools

The below links contain guides on installation of InfluxDB and Telegraf for performance monitoring:

a. https://docs.influxdata.com/influxdb/v2/install/?t=Linux InfluxDB

b. https://docs.influxdata.com/telegraf/v1/install/ Telegraf